
# NAVAL POSTGRADUATE SCHOOL

**MONTEREY, CALIFORNIA**

# THESIS

**IMPLEMENTING THE DOD JOINT OPERATION PLANNING PROCESS FOR PRIVATE INDUSTRY ENTERPRISE SECURITY**

by

Paul W. Poteete

September 2011

Thesis Advisor: Edward L. Fisher
Second Reader: Karl D. Pfeiffer

**Approved for public release; distribution is unlimited**

THIS PAGE INTENTIONALLY LEFT BLANK

| REPORT DOCUMENTATION PAGE | | | Form Approved OMB No. 0704-0188 |
|---|---|---|---|
| Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503. | | | |
| **1. AGENCY USE ONLY** ***(Leave blank)*** | **2. REPORT DATE** September 2011 | **3. REPORT TYPE AND DATES COVERED** Master's Thesis | |
| **4. TITLE AND SUBTITLE** Implementing the DoD Joint Operation Planning Process for Private Industry Enterprise Security | | **5. FUNDING NUMBERS** | |
| **6. AUTHOR(S)** Paul W. Poteete | | | |
| **7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)** Naval Postgraduate School Monterey, CA 93943-5000 | | **8. PERFORMING ORGANIZATION REPORT NUMBER** | |
| **9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES)** N/A | | **10. SPONSORING/MONITORING AGENCY REPORT NUMBER** | |
| **11. SUPPLEMENTARY NOTES** The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government. IRB Protocol number _____N/A_____. | | | |
| **12a. DISTRIBUTION / AVAILABILITY STATEMENT** Approved for public release; distribution is unlimited | | **12b. DISTRIBUTION CODE** | |

**13. ABSTRACT (maximum 200 words)**

The purpose of this research is to provide an analysis of the efficacy of the Joint Operation Planning Process (JOPP) to improve current enterprise security planning within the private industry. This report will investigate predominant frameworks used within private industry in order to define the purpose and weaknesses of each. The JOPP will be investigated to better understand what aspects may be viable for implementation into private industry enterprise security programs. This information will be used to develop a new process called the Enterprise Security Planning Process (ESPP) that will illustrate the potential use of the JOPP for private industry.

The conclusions derived through the research performed in this report are directed to the specific application of Department of Defense battle concepts into private industry security practices. The relevance of private industry's enterprise security programs to joint operation planning will be emphasized through the failures associated with the current business mindset of enterprise security operations. Private industry security operations will be illustrated as more closely related to military conflict than business-as-usual operations.

| **14. SUBJECT TERMS** Enterprise Security Framework, Joint Operation Planning Process (JOPP), Enterprise Security Planning Process | | | **15. NUMBER OF PAGES** 113 |
|---|---|---|---|
| | | | **16. PRICE CODE** |
| **17. SECURITY CLASSIFICATION OF REPORT** Unclassified | **18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified | **19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified | **20. LIMITATION OF ABSTRACT** UU |

NSN 7540-01-280-5500 Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

**Approved for public release; distribution is unlimited**

**IMPLEMENTING THE DOD JOINT OPERATION PLANNING PROCESS FOR PRIVATE INDUSTRY ENTERPRISE SECURITY**

Paul W. Poteete
Civilian, United States Navy
B.S., Excelsior College, 2002

Submitted in partial fulfillment of the
requirements for the degree of

**MASTER OF SCIENCE IN INFORMATION SYSTEMS AND OPERATIONS**

from the

**NAVAL POSTGRADUATE SCHOOL**
**September 2011**

Author: Paul W. Poteete

Approved by: Edward L. Fisher
Thesis Advisor

Karl D. Pfeiffer, PhD
Second Reader

Dan Boger, PhD
Chair, Department of Information Sciences

THIS PAGE INTENTIONALLY LEFT BLANK

# ABSTRACT

The purpose of this research is to provide an analysis of the efficacy of the Joint Operation Planning Process (JOPP) to improve current enterprise security planning within the private industry. This report will investigate predominant frameworks used within private industry in order to define the purpose and weaknesses of each. The JOPP will be investigated to better understand what aspects may be viable for implementation into private industry enterprise security programs. This information will be used to develop a new process called the Enterprise Security Planning Process (ESPP) that will illustrate the potential use of the JOPP for private industry.

The conclusions derived through the research performed in this report are directed to the specific application of Department of Defense battle concepts into private industry security practices. The relevance of private industry's enterprise security programs to joint operation planning will be emphasized through the failures associated with the current business mindset of enterprise security operations. Private industry security operations will be illustrated as more closely related to military conflict than business-as-usual operations.

THIS PAGE INTENTIONALLY LEFT BLANK

# TABLE OF CONTENTS

# LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

# LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

# LIST OF ACRONYMS AND ABBREVIATIONS

| | |
|---|---|
| BSI | British Standards Institution |
| ALE | Annual Loss Expectancy |
| ARO | Annual Rate of Occurrence |
| CC | Critical Capabilities |
| CCIR | Critical Commander's Intelligence Requirements |
| CIA | Confidentiality, Integrity, and Availability |
| CIO | Chief Information Officer |
| CISO | Chief Information Security Officer |
| CMM | Capability Maturity Model |
| CNO | Computer Network Operations |
| COA | Course of Action |
| CobiT | Control Objectives for Information and Related Technology |
| COG | Centers of Gravity |
| CR | Critical Requirements |
| CV | Critical Vulnerabilities |
| ESPP | Enterprise Security Planning Process |
| EW | Electronic Warfare |
| HIPPA | Health Insurance Portability and Protection Act |
| IEC | International Electrotechnical Commission |
| IO | Information Operations |
| ISACA | Information Systems Audit and Control Association |
| $(ISC)^2$ | International Information Systems Security Certification Consortium, Inc. |
| ISO | Industry Standards Organization |
| IT | Information Technology |
| ITIL | Information Technology Infrastructure Library |
| itSMF | Information Technology Service Management Forum |
| JIODPP | Joint Information Operations Defensive Planning Process |
| JOPP | The Joint Operation Planning Process |
| JOPES | Joint Operation Planning and Executive System |
| LOAC | Laws of Armed Conflict |
| MILDEC | Military Deception |
| MOE | Measures of Effectiveness |
| MOP | Measures of Performance |
| NIST | National Institute of Science and Technology Risk Management |
| RMF | Framework |
| OPSEC | Operations Security |
| PCI | Payment Card Industry |
| PCI-DSS | Payment Card Industry-Data Security Standards |

| | |
|---|---|
| PSYOP | Psychological Operations |
| ROE | Rules of Engagement |
| SEI | Software Engineering Institute |
| SLE | Single-Loss Expectancy |
| SP | Special Publications |
| TPI | Two-Person Integrity |

# ACKNOWLEDGMENTS

To my loving wife, Holly, and my children, Luke and Lisa. Without their support this would not have been possible. My sincere appreciation goes out to everyone on my thesis team.

THIS PAGE INTENTIONALLY LEFT BLANK

# I. INTRODUCTION

## A. OVERVIEW

This thesis will investigate the effectiveness of modeling long-range enterprise security planning after the Joint Operation Planning Process (JOPP) as currently implemented by the Department of Defense to better equip organizations to defend against physical, technical, and administrative security threats. Current enterprise security plans seem to fail to achieve functional viability due to a failure to: 1) understand that criminal- and terrorist-based attacks are better managed within a battlefield mindset than a business context, 2) properly organize the organization's staff through consistent security planning processes, 3) improve overly general technical recommendations that create both complexity and unending revision, 4) consider the risk facing the actual centers of gravity within an organization, and 5) adapt existing frameworks for crisis planning. This analysis will encompass security-planning methodologies for private-sector organizations and explore the current Department of Defense process in order to determine if the inadequacies of current security models may be improved upon through a more detailed application of the Joint Operation Planning Process. Overarching aspects of this investigation will include: identification of existing frameworks; the proper classification of security functions; strategic communications to include persuasion techniques for subsets of enterprise personnel that resist organizational goals; and deliberate crisis planning techniques.

The difficulty of conveying the nonbusiness nature of enterprise security, while aligning security with the business objectives, may lie within the rigid thinking surrounding business administration. Business and technical operations can be base-lined against pre-existing metrics such as system availability, units sold, customer satisfaction, and more.[1] System hardening and the fundamental organization of the business may change very little over the course of a few years. Enterprise security requirements may

[1] Kevin Behr, Gene Kim, and George Spafford, *The Visible Ops Handbook: Implementing ITIL in 4 Practical and Auditable Steps*, Eugene, Oregon: IT Process Institute, 2007, 4.

change by orders of magnitude from one hour to the next. This can be seen as an asymmetric conflict fought on the front lines of the company on a minute-by-minute basis. Although it is true that prevention, detection, and remediation systems far out-power the scanning "static" generated by immature attacks, it must be understood that robotic networks of computers (botnets), massive emailing of computer viruses, new phishing attacks, and advanced attack techniques can deliver serious challenges that require very technical and specific mitigation tactics. A skilled and creative staff and capable equipment are necessities for waging war against the onslaught of attacks that confront company assets on a daily basis.[2]

## B. THREATS

Security threats are continually increasing across the globe as firms have entered a marketplace without sovereign borders.[3] Enterprise security planning frameworks must extend beyond the technical business operations of organizations in order to address the risks to the core purpose of the firm. The current trend would indicate a gravitation of enterprise security offices to implement more complex management oversight based on regulatory and legal compliance initiatives.[4] This application of enterprise security controls to the sole attention of the legality and viability of business processes as seen within a market segment is woefully inadequate to manage the unstructured and asymmetric nature of today's security threats. It seems that the implementation of technical controls versus the institution of proper human involvement has also limited the ability for firms to react to crisis as incidents occur due to an over-reliance on consumer-off-the-shelf solutions. The increase of out-of-band and unconventional attacks against corporate entities will continue as information spillage, denial of service attacks prove to be effective means of funding terrorist entities, financial fraud, corporate espionage, and

---

[2] Douglas J. Landoll, *The Security Risk Assessment Handbook: A Complete Guide for Performing Security Risk Assessments* (New York, New York: Auerbach Publications, 2006), 45.

[3] John Rollins, Liana Sun Wyler, and Seth Rosen, "International Terrorism and Transnational Crime: Security Threats, U.S. Policy, and Considerations for Congress" (Congressional Research Service Report, January 2010), 13.

[4] Andrew Conry-Murray, "PCI And The Circle Of Blame," *Information Week*, 23 February 2008, http://www.informationweek.com/story/showArticle.jhtml?articleID=206800867 (accessed 3 March 2008).

other business impairment.[5] An analysis of how to determine the true Center of Gravity (COG) within a firm, persuade a population to meet the control objectives of a firm, properly define the controls required, and create intelligible plans that achieve the desired outcomes while providing for adaptation for disasters or crises is paramount to a firm's ability to adequately manage risk.

Information Security has become more of a battlefield than a business. Today's corporations face a multitude of attacks from malicious hackers, criminal organizations, terrorist organizations, and corrupt insiders.[6] All the while, a firm must be compliant with the most current regulatory requirements, moral obligations, and changes within society. The Joint Operation Planning Process (JOPP) offers some insight on the methods by which a firm can become aware of the true threats from malicious hackers and regulatory controls, develop a relevant strategy, institute a plan, and become responsive within a corporate structure that may be reticent to budget and implement enterprise security properly.

## C. ENTERPRISE SECURITY DEFINED

The purpose of enterprise security is not to eliminate the threat, but implement the level of protection required to maintain the preventive, detective, and corrective controls to mitigate loss to corporate resources.[7] The scope of security is determined by the management of confidentiality, integrity, and availability (see Figure 1) of its personnel, physical, and information assets.[8] This management is in response to threats that present the possibility that an entity may cause the assets to be degraded or disrupted in some way. This disruption to business productivity can come about by individual criminal acts, criminal organizations, foreign governments, competition, malicious hackers,

---

[5] Nick Bilton, "Hackers Claim to Have PlayStation Users' Card Data," *New York Times*, 28 April 2011, http://bits.blogs.nytimes.com/2011/04/28/hackers-claim-to-have-playstation-users-card-data/ (accessed 22 August 2011).

[6] John Rollins, Liana Sun Wyler, and Seth Rosen, "International Terrorism and Transnational Crime: Security Threats, U.S. Policy, and Considerations for Congress" (Congressional Research Service Report, January 2010), 13.

[7] Douglas J. Landoll, *The Security Risk Assessment Handbook: A Complete Guide for Performing Security Risk Assessments* (New York, New York: Auerbach Publications, 2006), 160.

[8] Ronald L. Krutz and Russell Dean Vines, *The CISSP Prep Guide: Gold Edition (*Indianapolis, Indiana: Wiley Publishing, 2003), 3.

malicious hacker activists (hacktivists), negligent employees, malicious programs, and ineffective or inefficient business processes. Regulatory compliance may also cause a loss of business productivity as business processes may need to be altered to fit within the new legal frameworks designed to guard against fraudulent, negligent, or illegal supply of the firm's products or services.

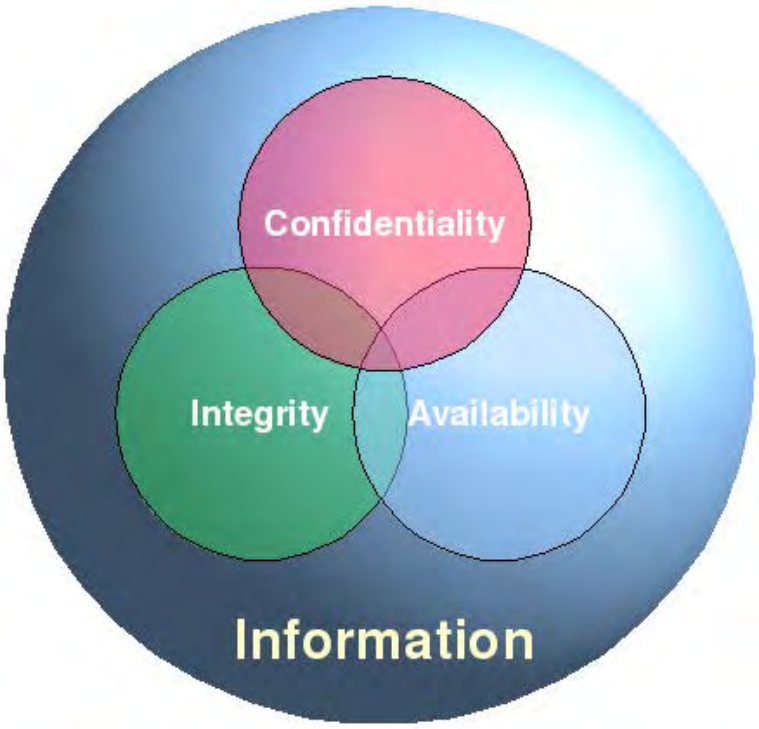



Figure 1. Information Security "CIA" Diagram

Threats are conducted by threat agents. These are entities or processes that conduct the malicious or generally destructive behavior. As with the aforementioned threats, threat agents may work for regulatory agencies, criminal organizations, or even the competition. The rise in technical speed and proliferation has also increased the incident of terrorist funding through the use of hacking techniques. The prevalence of both cyber-based terrorist funding and hacktivism activities from adversarial foreign governments underscores the necessity of viewing enterprise security programs as more battlefield than business.

Threats, through their related agents, impact systems through the exploitation of vulnerabilities. A vulnerability is a weakness in a person, system, or process that allows

for an adversarial force to disrupt, alter, destroy, or expose confidential information. The most common cause of exploitation of these weaknesses within a firm's personnel is through the use of social engineering or con-artistry.[9] In this case, the individual is fooled into exposing sensitive or confidential information. In some cases, physical violence or drugs may be used to extract information from the human target. This is not common within the corporate setting, but as terrorist funding and adversarial government entities increasingly target critical infrastructures, this may become more commonplace. Within a system, vulnerabilities are often encountered though programming flaws or weak authentication systems. These systems are often updated to guard against known exploitations on a regular basis; however, the use of poor authentication processes or methods can undermine the most secure system. Business process is often overlooked as a point of exploitation by malicious attackers; nevertheless, a business process can be manipulated in both legal and illegal contexts to disrupt business productivity.

Risk management is possibly the most important aspect of enterprise security planning. The probability of an incident through the exploitation of a vulnerability should be mitigated to a level that is deemed acceptable by the firm's senior management. The enterprise security office must understand the purpose of the firm and strategically align operations to mitigate, accept, or transfer the risks in a way that is financially responsible. The physical, information, and human assets of the organization, should be taken into consideration and assessed appropriately. This can be done using some common social network analysis techniques with impact or importance based on a measurement as simple as degrees of centrality (see Figure 2). In those cases, the degree of centrality possessed by a person or system should not be confused with a proper center of gravity analysis. The degree of centrality of the person or system can be used to aide the construction of a course of action, but it should not be mistakenly identified as the core purpose of the firm. In some cases, the detailed analysis of the systems themselves in relation to the risks facing the relevant vulnerabilities clouds the true intent of risk assessment. Risk is assessed as threats against the firm's productivity, not as simply the threats facing the complex systems therein. These risks not only fall within those that can

[9] Cyrus Peikari and Anton Chuvakin, *Security Warrior* (Sebatopol, CA: O'Reilly Media Inc., 2004), 209.

directly impact the immediate productivity of the firm, but can be realized through a damaged reputation, domestic irresponsibility, moral irresponsibility, or criminal negligence. The way in which a risk is both defined and addressed will be addressed within the context of the JOPP's center of gravity analysis.

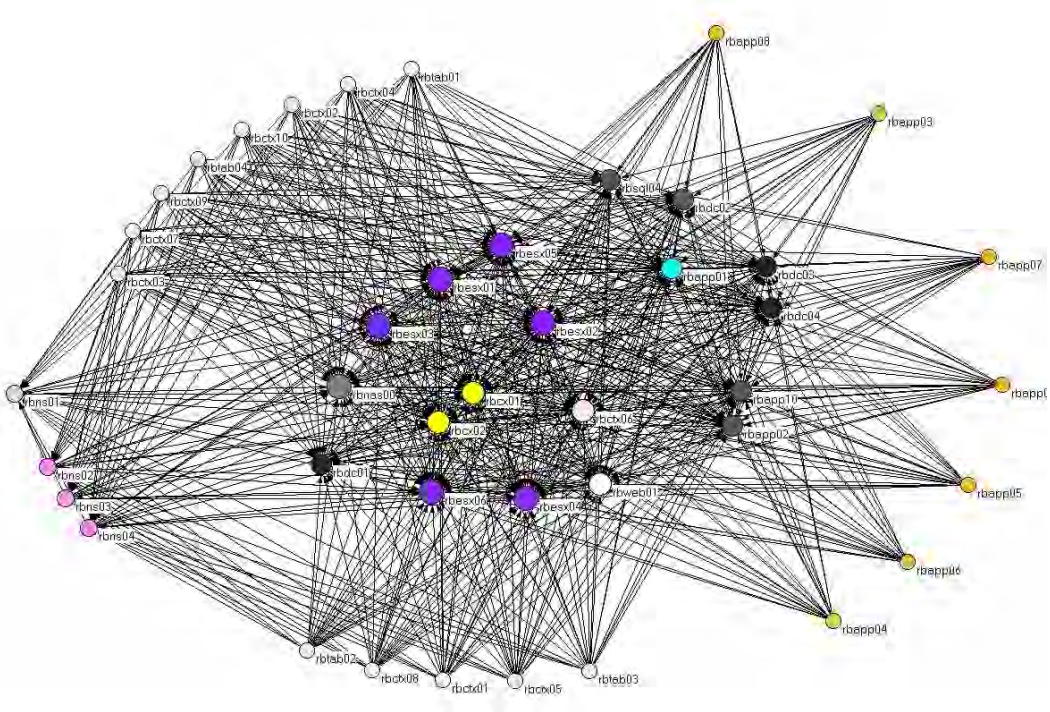



Figure 2. Citrix Interdependency Matrix

Beyond the identification of threats, exposures, and risk mitigation methodologies lies the crisis planning portion of enterprise security operations. These operations can be summarized as those activities dealing with the deterrence, protection, detection, and response to administrative, technical, and physical incidents. To expand on this topic, an enterprise security program should not only define the way in which a predictable situation is managed and measured, but it should account for situations for which the firm was unprepared. Many incidents can be foreseen as potentially occurring; therefore, at the very least, a rudimentary response can be crafted before the incident occurs. Some events are unpredictable and must be addressed as they arise. In these cases, it is important to identify if the anomaly is of malicious intent or random chance. Often, system anomalies are reported as malicious attack when they are actually no more than

poor configuration, human error, or an unrelated system error.[10] If the incident actually is malicious or of a recurrent nature, it should be contained and appropriately addressed. The fundamental aspect in dealing with incidents is not catching the culprit or repairing the broken information system, but restoring business productivity. If the business was not adversely impacted the incident can be addressed using methods that avoid disrupting other business processes or damaging the morale of the staff.

## D. ENTERPRISE SECURITY FRAMEWORKS

Currently, many industries depend on frameworks that require years of implementation and millions of dollars of human and industrial capital.[11] As with any well-developed plan, these frameworks offer a number of good ideas for how to manage enterprise security. An enterprise security framework is the method by which the security operations are managed within a firm. These frameworks often contain methods for physical, information, and data security operations; however, they will generally follow routine business processes to achieve their goals.

## E. JOINT OPERATION PLANNING PROCESS

The JOPP provides both a foundational and process-oriented approach to dealing with threats. The foundational aspects deal with strategy and the basics of communication. The JOPP has been used to manage large, complex, missions spanning multiple continents, cultures, and languages. The reduction of a process of such complexity into a subset of easily identifiable steps should be of great interest to

[10] Mason Pokladnik, "An Incident Handling Process for Small and Medium Businesses", SANS Institute InfoSec Reading Room, 2007, http://www.sans.org/reading_room/whitepapers/incident/incident-handling-process-small-medium-businesses_1791.

[11] Charles Robb, "Desperately Seeking Security Frameworks – A Roadmap for State CIOs," NASCIO, March 2009. http://www.nascio.org/publications/documents/NASCIO-SecurityFrameworks.pdf

enterprise security officers. The study and implementation of the concepts contained within this process can be of assistance to the effective and efficient management of an enterprise security program.

## F. ENTERPRISE SECURITY PLANNING PROCESS

The Enterprise Security Planning Process (ESPP) is created within this research as a solution that involves both the best aspects of current enterprise security frameworks, strategic communications as discussed in the context of information operations, and the Joint Operation Planning Process. The solution is presented as a method by which a firm can implement the JOPP to meet their enterprise security program needs. These programs will contain additional details that are not addressed directly within this research; nonetheless, effort is made to included appendices to better convey the intricacies of the more complex concepts.

## G. CONCLUSION

The following chapters will address an understanding of the growing security risks facing private organizations, the enterprise security frameworks used in corporations today, the Joint Operation Planning Process as currently used by the Department of Defense, the incorporation of the Joint Operation Planning Process techniques and principles as appropriate for unclassified use in medium to large organizations, and the proper establishment of enterprise architectures to meet the security threats facing these firms, with special consideration to the ability to properly identify the centers of gravity within the organization. The initial process will involve the study and review of information security threats facing critical infrastructures. A proper understanding of existing threats is essential to the analysis or development of a security framework. Successful analysis will be determined by the proper categorization of threats facing organizations and the incorporation of appropriate prevention, deterrent, and detection mechanisms to mitigate these risks.

An analysis of the current frameworks in use in corporations across the globe and an analysis of the Joint Operation Planning Process will provide for a foundational understanding of enterprise security planning. It is hoped that the analysis of current

frameworks for both private sector and Department of Defense entities will elucidate the shortcomings and positive attributes of each. This detailed clarification of the positive and negative principles will establish the foundational knowledge from which an analysis may be conducted.

The integration of the established principles will allow for the concise and clear construction of a new model developed through this research called the Enterprise Security Planning Process (ESPP) that may be instituted for effective enterprise security management. This model will be constructed in hope that it will be applicable in private-sector entities for the betterment of society through the implementation of business-driven enterprise security controls in a clear and effective manner with consideration to the applicability of the controls for deliberate planning as well as crisis objectives.

THIS PAGE INTENTIONALLY LEFT BLANK

# II. ENTERPRISE SECURITY PLANNING FRAMEWORKS

## A. MANAGEMENT PHILOSOPHY

As stated earlier, there exists a shortcoming in the correlation of incident prevention, detection, and response within corporate security operations.[12] This failure is further exacerbated by the improper focus of the security planning frameworks on which proper operations rely. The seamless integration of true security controls to meet business risk requirements is essential to the appropriate protection of firm assets.[13] This integration requires a strong understanding of the functionality provided by the operational units that compose the information security office. In the absence of this understanding, security officers may revert to a business management-oriented approach to the design and implementation of security frameworks. This approach ties much of the security program's success to business and management metrics, that when examined more closely, have little to do with the protection of information security assets.

It is true that the underlying systems must be well planned and implemented according to the appropriate business management methodology in use at the organization; however, the fundamental management philosophy of the firm should, and arguably must, be in place well before any comprehensive organizational structure would exist, and especially before a program as mature as a security framework is developed or integrated into the firm's business operations.[14] In the case of management philosophy, the military's approach to management standardization saves an enormous degree of frustration within a firm regarding what is classified as business appropriate and what would be a standing operating procedure. Even so, there is little evidence that any professional organization that would allow the continued employment of senior executives, or middle management for that matter, if they did not have a seemingly innate

12 Mark Story, "Sensible Security: Good Information Security is About Risk Awareness as Well as Sensible Investment in Automated Controls," *Management Today* (Sydney: Australia Institute of Management, 2008).

13 Ibid.

14 Chet Jernigan, "County and Municipal Government in North Carolina," The University of North Carolina at Chapel Hill, 2007.

understanding of proper business management. The reality is that a management philosophy is established well before the more mature organizational programs are instituted. In this vein, the problematic nature of management-centric security frameworks becomes increasingly evident.

In the words of an author regarding his book written to help managers interpret a single security framework for business use, he commented that his book "will save you months of work."[15] His book describes how to manage security governance for an organization, not the actual security of the organization. This underscores the lack of awareness surrounding the threats facing organizations from the core industries that manage the nation's critical infrastructure to the smaller businesses that may operate a hometown tax practice. Much of the time planning security operations within a firm is spent designing the management aspects of the underlying security organization, which should already be in place. Additional inspection into the International Information Systems Security Certification Consortium Inc. $(ISC)^{2'}$s "10 Security Domains," ISACA's "5 CISM Practice Areas," British Standards Institution's (BSI) Industry Standards Organization's (ISO) ISO 27001 (ISO 27002 defines the controls), and the IT Service Management Forum's Information Technology Infrastructure Library's (ITIL) guidance for integrating Information Technology (IT) services within a business spend a majority of their time discussing the bureaucratic structure required to manage the security infrastructure. For too long, the focus of security operations has been upon the proper institution of bureaucratic managerial systems to the detriment of the actual protection mechanisms that would provide meaningful security to an organization.

In some cases, the intractability of the senior management may be the most daunting obstacle working against the implementation of satisfactory security controls.[16] In this case, the onus is upon the information security officer's shoulders to properly convey the threats facing the firm and the methods by which these threats may be overcome. The overzealous nature of some security officers has led to a reticence among

---

15 "IT Governance's Complete ISO27001/ISO27002 Documentation Toolkit," *IT Governance*, 2005-2008 v7, www.itgovernance.co.uk.

16 NIST Special Publication 800-39, *Managing Information Security Risk Organization, Mission, and Information System View: Joint Task Force Transformation Initiative Information Security* (Gaithersburg, MD: National Institute of Standards and Technology, March 2011).

the executive staff to accept proposals relevant to firm security operations.[17] This hesitance to accept the program proposals is often due to a disconnection between the concepts of what is actually required versus the security proposal that has been submitted.

Executives in control of an organization's security may fall into three categories. The belief that all individuals in this role can be segregated into three roles is an over simplification, but it will serve to illustrate the problems currently facing the firms that manage the critical infrastructures of the United States. It is true that security and convenience do not go hand-in-hand, but there is an adequate middle-ground that can be achieved through a proper understanding of the threats, controls, and short-comings of security frameworks facing firms today. In the next few paragraphs the three categories will be discussed in more detail, with a final statement regarding the improper categorical allocation of time and resources within the most prevalent security frameworks.

### 1. Management-Oriented Security Professional

The first category of this discussion involves a management-oriented security professional that is overly interested in matching security controls to business processes. At the onset, this concept seems that it would be the most logical approach to the appropriate integration of security operations with business requirements; however, this is not the goal of this particular category of individual. The business-oriented professional is more keen on the proper interpretation of business outcomes than on the threats facing the firm's assets. This individual understands business processes, sales, revenue, risk mitigation, regulation, and the firm's varied practice areas. The management of vendors, contractors, and personnel are key for this individual, with negotiations and business contracts following at a close second place. The unpredictable disruption of business processes by malicious criminal organizations, adversarial governments, terrorist organizations, individual hackers, or loosely knit hacking activists (hacktivists) is unavoidable, and unfortunately, unexpected by this type of individual. This category has taken the time to plan for business-oriented approaches to known threats, with a disregard for the erratic nature of information security. The bottom line

[17] Laurie Kelly and John McCumber, *Assessing and Managing Security Risk in IT Systems: A Structured Methodology* (New York, New York: Auerbach Publications, 2005).

for this category of security professional is the proper documentation of security controls and the proper development of a formal business plan to address these controls. In reality, this individual's behavior is analogous to someone buying insurance for their home and locking the doors and windows when they are away. They fail to consider the possibility that a malevolent hacker may break the windows or destroy the foundation of the house to ruin or remove the contents. The firm's reputation would be tarnished to a point of total loss, but the paperwork would be sufficient for almost any regulatory requirement.

### 2. Security-Centric Professional

The next category of security professional in this discussion will be called the security-centric professional. This individual is overly concerned with mitigating the risks facing the organization. This category involves a team whose sole purpose is to identify and remove every potential threat from an organization. The policies that are common within this category involves everything from the requirement of the company to monitor an employee's personal use of the Internet within their own home, the scrutiny of meaning behind employee blog comments, personal statements, and family members, to the complete annexation of company-owned equipment for approved business purposes only. There are companies that would not allow the use of any application, including word processors, without the explicit approval of the firm's finance office with the appropriate allocation of budget codes. This can cascade into the types of cell phones, computers, cameras, copiers, and fax machines that employees are allowed to use at their private homes. This individual is not concerned with accomplishing the organization's mission, but only with the most secure method by which these systems may be utilized within the firm. Usability is lost to security. This individual's program could be analogous to the house that is encased in lead, then concrete, and then thoroughly setup with proximity alarms at the only entrance. The difficulty of maintaining security thwarts business productivity. This office believes that every aspect of the business should be mathematically definable and planned accordingly. As absurd as it sounds, the prevalence of this type of thinking is becoming more commonplace in management and engineering professions. The idea that all variables already exist and

can actually be counted, ascribed to a meaning, and correlated to a business or security purpose is flawed. Whether this concept comes from the educational system regarding evolutionary concepts that cannot be questioned or scientific principles that are beyond reproach, it is not clear. What is clear, is that this concept damages the bottom line of an organization by preventing or limiting useful output.

### 3. Joint Operations Security Professional

The final category in this illustration is the joint operations security professional that uses the proper combination of the multiple facets contain within the information security domains and practice areas. This understanding allows for the effective coordination of distinct administrative, technical, and physical resources and capabilities to develop a proper system capable of defining the security operations of the firm. This posture is determined through a skilled examination of the threats facing the firm's assets, the vulnerabilities inherent to, or injected into, these assets, and the protection mechanisms that are appropriate to meet the firm's tolerance for the risk associated to these assets. To understand this relationship, a joint operations approach not only takes into account the management of the system, but allows for the response to unexpected input. As will be discussed in later chapters, this will involve the incorporation of critical information requirements regarding the firm's goals, an analysis of the impact resulting from the exploitation of existing or created vulnerabilities in firm assets, and proper measures of performance and effectiveness in regard to the mission at hand. This professional's philosophy can be best likened to the concept, "Don't sweat the small stuff."[18] This individual takes the time to understand the most important operations and systems within the firm. This virtual inventory is thoroughly examined for vulnerabilities. This knowledge is combined with an expert awareness of the threats that exist and how they would exploit vulnerabilities in the firm's systems. These metrics are then used to develop or acquire the appropriate protection mechanisms that provide the most effective means of reducing the impact of malicious, disastrous, errant, or negligent activity to meet the firm's risk tolerance. A solid understanding of the industry's most

[18] Richard Carlson, *Don't Sweat the Small Stuff and It's All Small Stuff: Simple Ways to Keep the Little Things from Taking Over Your Life* (New York, New York: Hyperion Books, 1997), 89.

prevalent approaches to information security, the threats facing organizations today, and the joint operation planning process provides this professional with a solid foundation to secure an organizations personnel, facilities, and information.

## B. OPERATIONAL SECURITY FRAMEWORKS

Currently, many industries depend on one of the many prevalent operational security frameworks to manage their information security activities.[19] There are several additional frameworks that are worthy of comparison and discussion, but predominately, the Industry Standards Organization (ISO), Payment Card Industry (PCI), the Information Systems Audit and Control Association (ISACA), and the Information Technology Service Management Forum (itSMF) are the organizations leading framework development around the globe. Deficiencies in the frameworks developed by these organizations will be discussed throughout each section; however, the primary goal of this section is not to merely define the problems within the program, but to also convey the primary organizational objective promoted by each framework. As with any well-developed organizational plan, there is a great deal to learn from studying these frameworks and their associated ideological exhortations. Much of the information contained within each framework is very relevant to the enterprise security needs of firms across the globe. Having implemented any of these frameworks, a firm could expect to achieve a more capable posture in protecting their assets.

An enterprise security framework could be defined as being a combination of methodology and procedure for governing the enterprise security operations of a firm or organization.[20] This would include the overarching concepts surrounding the risks facing administrative, technical, and physical assets within the firm, as well as a solution geared to address each area. As the capabilities and features offered by industry increase and become more complex, so must the security program evolve. The security landscape has

[19] Charles Robb, "Desperately Seeking Security Frameworks – A Roadmap for State CIOs," NASCIO. March 2009, Accessed July 17 2011. http://www.nascio.org/publications/documents/NASCIO-SecurityFrameworks.pdf.

[20] Ibid.

changed in the last decade, allowing exploits to be introduced at incredible speeds.[21] This puts pressure on the security function of a firm to become increasingly agile and adaptable to the ever-changing topography. Enterprise security frameworks must rely on concepts more appropriate for a battlefield scenario than that of a business. Corporations face a multitude of threats from malicious hackers, criminal organizations, terrorist organizations, and corrupt insiders. All the while, a firm must be compliant with the most current regulatory requirements. Enterprise security frameworks should enable the balance between business process and security capability, while maintaining extreme agility. In most cases, regulation trumps reality.

As evidenced by current events in the media and within the information security community, the most prevalent security frameworks lack the core identification of what is truly important to a corporation's security.[22] This is exacerbated by a lack of examination of the techniques required for organizing differing departments to produce a successful security operation. It would appear that more often than not, the introduction of a security framework provides a regulatory barrier to divert blame or simply inflate capabilities to appease client concerns. It is repeatedly reported that the overwhelming detail required to implement many frameworks will take a well-organized firm years of concerted effort to merely establish the program and many more to build a monitoring and reporting system to take advantage of it.[23] Over the next few sections, four prominent security frameworks will be discussed, with special attention paid to the primary focus of each framework, its use in an enterprise, noteworthy deficiencies. In the future chapters, a more direct review of when and where the Joint Operation Planning Process could be introduced to alleviate many of these shortfalls will be discussed.

---

[21] "Lumension Scan," April 2009, http://www.lumension.com/vulnerability-management/vulnerability-assessment-software.aspx (accessed July 2011).

[22] Steve Ragan, "Does the Heartland Breach Prove PCI Useless?," 26 January 2009, http://www.thetechherald.com/article.php/200905/2849/Does-the-Heartland-breach-prove-PCI-useless (accessed 18 August 2011).

[23] Charles Robb, "Desperately Seeking Security Frameworks – A Roadmap for State CIOs," NASCIO, March 2009, 3.

### 1. British Standards Institution (BSI) International Organization for Standardization's 27001 Framework (ISO/IEC 27001:2005)[24]

As the most comprehensive and mature framework used in the private sector, the ISO 27001 framework is considered a daunting, overly bureaucratic standard whose comprehensive implementation would bring any firm's security operations to a crawl.[25] It was developed by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) in October 2005 as a replacement for the British Standards Institution's BS7799, developed in 1995. Implementation of the ISO 27001 framework allows an enterprise to receive ISO 27001 Certification, which, in turn, allows for audits and formal compliance certificates. The goal of the program is to establish a cohesive and integrated approach to managing information security requirements. The program is comprised of approximately 13 primary security management categories with over 200 subcategories (Table 1). Throughout the entirety of the published framework, there is no reference to what would be considered an actual security control mechanism. There is no mention of how, when, where, or why to implement firewalls, identity management systems, door locks, or even security awareness programs. There are three sections that refer to the proper use of passwords and another section discussing the importance of clock synchronization. The framework also provides for three levels of auditing by means of the formal certification standard. The stages are designed to audit the firm's compliance with the framework at increasingly demanding levels of difficulty. This is a profitable option for firms offering auditing services for the ISO 27001 certification.

[24] Alberto Bastos and Rosangela Caubit, ISO 27001 and 27002: Information Security Management (Atlanta, GA: Módulo Security Solutions, 2010).

[25] Dejan Kosutic, "Main obstacles to the implementation of ISO 27001," 1 June 2010, https://www.infosecisland.com/blogview/4205-Main-obstacles-to-the-implementation-of-ISO-27001.html.

| Primary Security Management Categories |
| --- |
| Structure |
| Risk Assessment and Treatment |
| Security Policy |
| Organization of Information Security |
| Asset Management |
| Human Resources Security |
| Physical Security |
| Communications and Ops Management |
| Access Control |
| Information Systems Acquisition, Development, Maintenance |
| Information Security Incident management |
| Business Continuity |
| Compliance |

Table 1. Primary Security Management Categories[26]

The primary deficiency perceived within this framework is its indomitable size and complexity. In a publication written in 2009, Charles Robb reported that the program took most businesses over a year to implement, requiring numerous additional years to develop for management and monitoring systems that were capable of auditing the project.[27] Due to the vague nature of much of the framework, endless checklists could be developed to provide assistance with its continued management. Perhaps the most intriguing aspect is the amount of data that the certified firms are losing. Many of the recipients of the ISO 27000 series certification were at the top of the list of companies that have experienced the most devastating security breaches in the history of the Internet. This list includes: 90,000 records lost from Booz Allen Hamilton; 90,000,000

[26] ISO/IEC 27002, 19 December 2010, http://en.wikipedia.org/w/index.php?oldid=403171569 (accessed 16 January 2011).

[27] Charles Robb, "Desperately Seeking Security Frameworks – A Roadmap for State CIOs," NASCIO, March 2009, 3.

records lost from TRW; 90,000,000 records lost from Sears Roebuck; 77,000,000 records lost from Sony Corporation; and 25,000,000 records lost from HM Revenue and Customs.[28, 29]

Overall, this program attempts to continuously grow a program centered in bureaucratic management of information systems and corporate process. The increasingly long duration required to implement this framework, coupled with the diminishing amount of time in which new security exploits are uncovered and introduced into the wild, makes for a complicated proposal regarding the viability of such an investment. This daunting framework also leaves the identification, selection, and methods for the proper implementation of most technical controls up to the enterprise itself. This is certainly not to say that an enterprise security framework should provide a technical procedure manual for vendor-specific security appliances and software, but it should certainly provide for the base capabilities. After years of considering the options regarding various security frameworks available to private industry, firms believe that a solution should be available that both provides for a straightforward method for integration into the existing management operations and culture, and improves the enterprise security infrastructure for which it was acquired.

### 2. Payment Card Industry – Data Security Standards (PCI-DSS)[30] [31]

Possibly the most comprehensible framework is the PCI-DSS, which, in reality, is not a formal framework at all, but a cohesive set of security standards designed to aid merchants who accept credit cards properly manage their security operations. Created in December 2004, this framework was developed through a joint venture between a few large credit card processors, American Express, Discover Financial Services, JCB, MasterCard Worldwide, and Visa International.[32] As of version 2.0, the PCI-DSS

---

[28] Dataloss Database, *Open Security Foundation*, 2011, http://datalossdb.org/index/latest.

[29] ISO Certification List, *British Standards Institution*, http://www.bsigroup.com/en/Assessment-and-certification-services/Client-directory/CertificateClient-Directory-Search/Post.aspx?id=88254&epslanguage=EN (accessed 1 July 2011).

[30] PCI-DSS., http://en.wikipedia.org/wiki/Payment_Card_Industry_Data_Security_Standard.

[31] *PCI DSS Requirements and Security Assessment Procedures, Version 2.0 (October 2010).*

[32] PCI-DSS FAQs, *GFI Software*, http://www.gfi.com/security/pcifaqs.htm.

framework provides for twelve primary requirements ranging from firewall configuration to policy development (Table 2). These requirements are further developed through the incorporation of approximately 426 defining aspects that further aid the merchant in compliance with the primary goals. The local banks, which operate merchant accounts, process the credit card transactions for the credit card processor. This security standard provides a, mostly, straightforward method to manage their security operations.

| PCI-DSS Framework |
|---|
| Requirement 1: Install and maintain a firewall configuration to protect cardholder data |
| Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters |
| Requirement 3: Protect stored cardholder data |
| Requirement 4: Encrypt transmission of cardholder data across open, public networks |
| Requirement 5: Use and regularly update anti-virus software or programs |
| Requirement 6: Develop and maintain secure systems and applications |
| Requirement 7: Restrict access to cardholder data by business need to know |
| Requirement 8: Assign a unique ID to each person with computer access |
| Requirement 9: Restrict physical access to cardholder data |
| Requirement 10: Track and monitor all access to network resources and cardholder data |
| Requirement 11: Regularly test security systems and processes. |
| Requirement 12: Maintain a policy that addresses information security for all personnel. |

Table 2. PCI-DSS Framework[33]

As with any private sector program developed by the banking industry, there are some interesting caveats regarding the true intentions of the program. It has been said that the PCI-DSS requirement is actually so strict as to be unachievable, allowing for what has been touted as "The PCI-DSS Blame Game" causing all monetary damages to be deflected back to the local merchant.[34] Any failure to meet all of the requirements presented in the PCI-DSS standard allows for the credit card processor to divert monetary damages back to the credit card merchant account, who originally processed the request. The breach implications are teamed with additional benefits and fines. PCI-DSS also provides justification to move a merchant account up or down a credit processing scale.

[33] *PCI DSS Requirements and Security Assessment Procedures, Version 2.0 (October 2010), 3.*

[34] Andrew Conry-Murray, "PCI And The Circle Of Blame," *Information Week*, 23 February 2008, http://www.informationweek.com/story/showArticle.jhtml?articleID=206800867 (accessed 3 March 2008).

At the top-end of the scale, the merchant is said to be in full compliance with PCI-DSS; therefore, the merchant would receive the benefit of lower transaction fees and reduced monthly recurring fees. At the bottom-end of the scale, the merchant would be required to pay a premium to provide credit card processing to their clients and would be forced to pay additional monthly recurring fees. This not only affects the per transaction and recurring fees associated with providing credit card processing services, but it provides for the credit card processor a method by which to associate the legal and financial implications of a breach to the local merchant account. This is an improvement for the credit card processor, as for many years fraudulent charges were a liability to the main processor and not the local merchant account. This now allows the large credit card processing entities to avoid losses from credit card fraud or system exploitation.

Primarily, the focus on legal and financial repudiation, the increasingly specific requirements, and the failure to address departmental interoperability issues surrounding organizational security operations plagues this framework. The requirements range from the type and length of a password to the duration that a system may operate without a patch. In many cases these requirements are moot or unnecessarily restrictive. Many of the requirements would be analogous to requiring a 300 meter water resistance certification for global positioning satellite hardware; however, failure to meet the requirements, even the useless ones, may result in otherwise unpreventable fraudulent actions being legally attributable to the local merchant account. This focus on the legal versus the necessary may be evidenced in the data loss statistics, which report that the security standards used in creating the PCI-DSS framework did not prevent CardSystems, Visa, MasterCard, and American Express from losing 40,000,000 records in 2005.[35,36] This, coupled with the stringent, yet sometimes useless technical requirements, makes for various interpretations of the real purpose behind the PCI-DSS. Moving beyond the legal and financial penalties, the lack of joint departmental support within the program can result in process duplication or inattention. Whereas the duplication of effort may only create inefficiencies and personnel conflicts, the nonexecution of security controls may

35 Andrew Conry-Murray, "PCI And The Circle Of Blame," *Information Week*, 23 February 2008, http://www.informationweek.com/story/showArticle.jhtml?articleID=206800867 (accessed 3 March 2008).

36 Dataloss Database, *Open Security Foundation*, 2011. http://datalossdb.org/index/latest (accessed July 2011).

result in unauthorized disclosure, alteration, or unavailability of organizational assets. These failures could result in irreparable harm to the company. Additional attention may be brought to what the PCI-DSS calls, "Compensating Controls." These are exceptions to the programs requirements that are officially allowed by the auditor or card processor. These controls allow for businesses to fall short in some areas and still receive a stamp of approval for business practices.

### 3. Information Technology Service Management Forum's (itSMF) Information Technology Infrastructure Library (ITIL)[37]

The final two frameworks in this discussion move further from enterprise security planning and operations into the realm of general information technology governance. They are included in the enterprise security analysis, as they are commonly used to both manage enterprise technology and enterprise security. In this case, the former application is properly applied, whereas the latter is somewhat inadequate to meet the needs of today's security landscape. The first of these two frameworks is ITIL. ITIL was originally designed by the British Central Computer and Telecommunications Agency to provide a system by which organizations could create cohesive information technology management operations to provide for customer service. Originally, in the mid-1990s, ITIL was composed of thirty volumes. The massive information overhead associated with beginning an ITIL-based process led the newly established Office of Government Commerce to reduce the publication to eight logical volumes. The volumes define four phases for IT service management under which there are approximately forty auxiliary objectives (Table 3).

| ITIL Phases |
| --- |
| Phase One: "Stabilize The Patient" And "Modify First Response" |
| Phase Two: "Catch & Release" And "Find Fragile Artifacts" Projects |
| Phase Three: Create A Repeatable Build Library |
| Phase Four: Continual Improvement |

Table 3. ITIL Phases[38]

[37] Kevin Behr, Gene Kim, and George Spafford, *The Visible Ops Handbook: Implementing ITIL in 4 Practical and Auditable Steps* (Eugene, Oregon: IT Process Institute, 2007), 25-64.

[38] Ibid.

The primary goal of ITIL is to provide a service-centric model for corporations and government entities to provide business services of the best quality and appropriate quantity. Many organizations that subscribe to the ITIL methodology for IT management have also attempted to apply this framework to their security programs. Unfortunately, the ITIL framework is poorly designed for this purpose, and may event cause rifts within the information technology division itself.[39] The fundamental problem with enforcing ITIL within an enterprise security infrastructure is the misallocation of resources and inappropriate benchmarking. The metrics used to measure the effectiveness within the ITIL framework surround capacity management, service continuity, customer response ratings, configuration management, and freezing operations until proper management is implemented. These are very positive goals for any information technology department, but information security requires both agility and highly skilled personnel. Thorough documentation of business processes will never be an acceptable alternative to having individuals who can make decisions and think through complex situations.

The primary shortcomings in using ITIL as a framework for enterprise security operations are that it lacks virtually every security control and process known and that it creates a bureaucratic system that limits individual responsibility.[40] ITIL establishes control review boards for most projects and configuration modifications. No one person is permitted complete control over any system.[41] Whereas Two-Person Integrity (TPI) is a necessary solution when considering the employment of a nuclear weapon, it is poorly suited for the daily operations of an enterprise security division. It could be argued that it is a bad solution for the management of information technology departments, as well. Security operations can require a level of agility that is impossible to achieve when a operational review board is required for each decision. This framework is best suited for individuals who do not have access to the underlying technical architecture of the enterprise or its security infrastructure. The engineers and architects that design and

39 John Wallhoff. *ITIL Security Management* Presentation, May 2005, http://www.scillani.se/assets/pdf/Scillani%20Presentation%20ITIL%20Security%20Managment.pdf (accessed 1 July 2011).

40 Ibid.

41 Kevin Behr, Gene Kim, and George Spafford, *The Visible Ops Handbook: Implementing ITIL in 4 Practical and Auditable Steps* (Eugene, Oregon: IT Process Institute, 2007), 25–64.

manage these should be held responsible for their actions because they probably already possess a level of maturity that comes with the experience required to reach a high level of responsibility. The detective controls indicated in this framework underscore the difficulty adhering to the program. This can be exemplified in one corporate example where the increased complexity caused by implementing the ITIL framework did untold damage to the corporation's bottom line. A manager rolled-out the ITIL change management process by using the recommend change control review board. This is a group of individuals that must read and approve all changes submitted by the technical staff. The review board may possess less knowledge concerning the impact of the change than the technician submitting the request. The corporation found that the inefficiency created by the program was so great that the information technology staff was required to circumvent the framework to maintain fundamental corporate operations. The management staff did not interpret the circumvention as a necessity to keep the business operational, but enforced the zero-tolerance policy in respect to using the change control review board that had been established. There was no data available to document what occurred after the zero-tolerance policy regarding the change control review board was enforced, but it would be conceivable that the firm ceased to exist.

### 4. Information Systems Audit and Control Association (ISACA) Control Objectives for Information and Related Technology (CobiT)[42]

CobiT will be the final framework used to illustrate the need for a new methodology of managing enterprise security. CobiT is, once again, not specifically designed with enterprise security infrastructures in mind; nonetheless, many firms are using it as the primary source for enterprise security planning around the world. Much of the misapplication of the previous mentioned frameworks can be traced back to an unsatisfactory understanding of the difference between the battlefield of enterprise security operations as compared to standard information technology operations.

CobiT was designed by what is now ISACA in 1994 to establish a cohesive means by which the technical operations of a corporation could be governed. The predominant focus regards the proper understanding of business needs, as fulfilled by

[42] CobiT 4.1 (Rolling Meadows, IL: IT Governance Institute, 2007).

technical solutions in the most efficient way possible. It is comprised of four primary categories over thirty-four (Table 4) defined processes that are rated using the Software Engineering Institute's (SEI's) Capability Maturity Model (CMM). Even though the CobiT framework is highly complex and comprehensive, it still calls on the following standards for additional content:

- ITIL for service delivery
- CMM for solution delivery
- ISO 17799 for information security
- PMBOK or PRINCE2 for project management.

Even though ISACA admitted that CobiT is not adequate for enterprise security governance, this does not seem to affect the decision of corporations to continue to implement security systems by way of CobiT. Risk is the primary concern for corporate security, and risk has traditionally been managed using business process against definable variables. Mitigating risk has been a calculated business program, not the rugged battle plan proposed in this research. There is always a risk associated with bringing a new product to market. The community may also reject changes in color, flavor, or function of existing products. Predictions made regarding the Stock Market or other financial obligations can sometimes be mitigated by a single department or contract. The CobiT framework is more of a system management philosophy or foundational instructional guide. It certainly should not be considered a solution for the joint incorporation of business resources to prevent and respond to malicious attack.

**CobiT**

| **4 Primary Categories:** |
|---|
| Plan and Organize |
| Acquire and Implement |
| Deliver and Support |
| Monitor and Evaluate |

| **Plan and Organize:** |
|---|
| PO1 Define a strategic IT plan. |
| PO2 Define the information architecture. |
| PO3 Determine technological direction. |
| PO4 Define the IT processes, organization and relationships. |
| PO5 Manage the IT investment. |
| PO6 Communicate management aims and direction. |
| PO7 Manage IT human resources. |
| PO8 Manage quality. |
| PO9 Assess and manage IT risks. |
| PO10 Manage projects. |

| **Acquire and Implement:** |
|---|
| AI1 Identify automated solutions. |
| AI2 Acquire and maintain application software. |
| AI3 Acquire and maintain technology infrastructure. |
| AI4 Enable operation and use. |
| AI5 Procure IT resources. |
| AI6 Manage changes. |
| AI7 Install and accredit solutions and changes. |

| **Deliver and Support:** |
|---|
| DS1 Define and manage service levels. |
| DS2 Manage third-party services. |
| DS3 Manage performance and capacity. |
| DS4 Ensure continuous service. |
| DS5 Ensure systems security. |
| DS6 Identify and allocate costs. |
| DS7 Educate and train users. |
| DS8 Manage service desk and incidents. |
| DS9 Manage the configuration. |
| DS10 Manage problems. |
| DS11 Manage data. |
| DS12 Manage the physical environment. |
| DS13 Manage operations. |

| **Monitor and Evaluate:** |
|---|
| ME1 Monitor and evaluate IT performance. |
| ME2 Monitor and evaluate internal control. |
| ME3 Ensure compliance with external requirements. |
| ME4 Provide IT governance. |

| **SEI CMM:** |
|---|
| Level 0: Non-existent |
| Level 1: Initial/ad hoc |
| Level 2: Repeatable but Intuitive |
| Level 3: Defined Process |
| Level 4: Managed and Measurable |
| Level 5: Optimized |

Table 4. CobiT Framework[43]

[43] *COBIT 4.1* (Rolling Meadows, IL: IT Governance Institute, 2007), 26.

The National Institute of Science and Technology Risk Management Framework (NIST RMF) deserves some mention as it is composed of over 1,323 pages of resources that can be used to develop an information security framework.[44] The NIST methodologies started as a program to aid the health care industry with the Health Insurance Portability and Protection Act (HIPPA). Regardless of the initial purpose, the methodologies are useful across any industry desiring to augment their understanding of security controls and methodologies. A NIST RMF implementation methodology is now under development; however, the use of the RMF as an industry standard framework has not taken hold. Even so, the individual NIST Special Publications (SP) that compose the RMF are widely used in the development of alternative frameworks across multiple disciplines. The reservation regarding NIST RMF implementation as the guiding framework may be related to the tens of thousands of pages of policies, standards, guidelines, and procedures that NIST has produced over the years. In this case, it is not the failure to provide an adequate information repository for its advocates, but an overload of information. It is clear that the methodologies and principles developed and endorsed by NIST will continue to be a driving force in the advancement of understanding information security; nonetheless, the concerted implementation of the comprehensive NIST RMF may still remain a noble academic exercise for the foreseeable future.

## C. SECURITY FRAMEWORK SOLUTION

The four frameworks mentioned above are the predominate forces in corporate America. These are the standards and frameworks that Chief Information Officers (CIOs) and, sadly, Chief Information Security Officers (CISOs) see as comprehensive solutions for enterprise security governance. More often than not, these frameworks may further complicate an already complicated situation, concealing the program deficiencies through excessive reporting and bureaucratic overhead. This problem is further augmented by the detailed complexity in the reporting systems themselves. A

[44] NIST RMF Documents: FIPS-PUB-199-final.pdf, FIPS-PUB-200-final-march.pdf, Risk-Management-Framework-2009.pdf, SP800-18-rev1-final, SP800-30, SP800-37-rev1-final, SP800-39-final, SP800-53A-rev1-final, SP800-53, SP800-59, SP800-60_Vol1-Rev1, SP800-60_Vol2-Rev1 (2011).

department could spend a month of concerted effort to produce a weekly report. The weekly report that is produced is not only almost a month behind schedule, but it really does not reflect reality in the first place. A common sense methodology that incorporates the joint requirements and capabilities of the business's various units is needed to combat this aggravating dilemma. A solution that takes into consideration the requirements, functionality, and interoperability to produce a verifiable course of action that maintains the agility required to combat intermittent and unexpected threats is a necessity.

It has been said that employees are the biggest threat to a firm's security.[45] If this is the case, then move the firm's confidential records to the sidewalk, away from the employees, and monitor the firm's progress from there; nonetheless, if the executive management is leaning on the already mentioned frameworks to provide a solution for enterprise security governance, than it might just be true.

[45] Eric Cole and Sandra Ring, *Insider Threat: Protecting the Enterprise from Sabotage, Spying, and Theft (*Waltham, Massachusetts: Syngress, 2006), 8.

THIS PAGE INTENTIONALLY LEFT BLANK

# III. THE JOINT OPERATION PLANNING PROCESS AND INFORMATION OPERATIONS FOR CORPORATIONS

## A. INTRODUCTION

Many of the failures associated with enterprise security planning frameworks and operations may revolve around the interpretation of enterprise security activities into business management concepts. The conceptual risk framework designed for overt and legitimate business transactions often does not meet the criteria for circumstances that arise as the result of illegal actions. Beyond risk management, failures are associated with the unification of effort, the clear delineation of objectives, the proper allocation of resources to tasks, and appropriate communications among teams.

Within enterprise security, there are three key concepts that represent areas with the highest probability of failure: 1) Understanding, 2) Planning, and 3) Communication. Core capabilities must be centered within these key areas to produce a viable enterprise security plan.[46] A failure within any of these key areas will result in the inability for an organization to maintain adequate levels of security. In such cases, corporations must abandon risk mitigation and accept the higher cost of risk transfer to insurance options to meet the basic requirements for regulatory compliance and the impending litigation that will occur due to the lack of reasonable procedures. Primarily, this chapter will investigate the Joint Operation Planning Process as it is involved within Information Operations to create a planning and communications process that is capable of meeting the requirements for a successful enterprise security program.

In many instances, corporations lack the requisite skills needed to ascertain whether a security professional is capable to meet the requirements of the job. As a result, corporations have regressed to standard business management concepts surrounding common regulatory definitions of risk management and organizational

46 "Poor Understanding Of Information Security Risk At Many Firms, Survey Finds," April 2011, http://www.infosecurity-us.com/view/17368/poor-understanding-of-information-security-risk-at-many-firms-survey-finds/ (accessed 1 August 2011).

liability. Corporations will commonly attempt to convey their needs in general terms such as confidentiality, integrity, availability, the reduction of vulnerabilities, and compliance. In such cases, a reliance on certifications and academic credentials will assist in the process, but even these aspects will require an interviewer that possess the skill to determine if an individual has an actual understanding of the concept described in the job description. In these cases, employment outsourcing firms may provide organizations with the tools needed for the proper acquisition of talent.

Beyond the foundational knowledge required to lead information security operations, the ability to conduct proper planning within an organization to implement security controls to meet organizational mission objectives is critical. To better understand the relationship that will be drawn between the previous chapter and this chapter, Information Operations components and the Joint Operation Planning Process will be summarized. The summaries will attempt to provide an overview of the military's current conceptual framework, while drawing from some private industry concepts of similar activities.

## B. THE JOINT OPERATION PLANNING PROCESS

> War plans cover every aspect of a war, and weave them all into a single operation that must have a single, ultimate objective in which all particular aims are reconciled. No one starts a war or rather, no one ought to do so without first being clear in his mind what he intends to achieve by that war and how he intends to conduct it.[47]

The Joint Operation Planning Process (JOPP) provides a straightforward process for the development of effective mission orders. National operations are complex, joint operations conducted through and within foreign territories, and in conjunction with allied or friendly foreign nationals achieve levels of daunting complexity. The JOPP takes a portion of a complex process and reduces it to the most critical components necessary to meet the mission objectives at hand. From initiation to final plan

[47] Carl von Clausewitz, *On War* (London, England: Penguin Group, 1982. First published 1832 by Vom Kriege), chapter 2.

development, the commander exercises strategic control and communication, while entrusting subordinate and cooperative commands with their mission objectives. The process, as defined below, does require several fundamental concepts to be understood and acted upon by the initiating command throughout the operations. The reduced complexity of this process still exceeds the requirements of an enterprise security framework instituted within a large corporation. Due to the dynamic environment in which military operations are conducted, it is necessary that some concepts contained within the JOPP are excluded to better lay a foundation for the creation of a private-sector enterprise security framework and planning process.

A mission of any complexity cannot be completed without the vision and strategic direction of the commander. The commander must have a solid understanding of the task to be accomplished and must clearly convey this message to the forces involved. This communication should be orchestrated in such a way as to both reinforce the purpose of the mission, and garner widespread support. To gain support the message should be crafted in clear terms and through subtle persuasion. The vision should be communicated in a way that conveys the message with utmost accuracy and does not generate excessive damage to morale. Having established the strategic direction, established the proper staffing and command relationship channels, and having created a system by which the commander can conduct strategic communications throughout the entire mission, the process may begin.

At the beginning of the process, there must be a subset of capabilities communicated to the forces involved. The strategy and concept of battle will set the stage from which the command will begin the planning process. An overall view of this procedure brings the strategic guidance and mission concept to the creation of a plan. Within the planning process, refinement, adaptations, and the decision to abort or to proceed with the mission are conducted.[48]

[48] *Joint Operation* Planning: Joint Publication 5-0. (26 December 2006), III-5.

1. Strategic Guidance.

2. Concept Development.

3. Plan Development.

4. Plan Assessment (Refine, Adapt, Terminate, Execute).

In order to pick concepts that best suit the case analysis relating to enterprise security, portions of the JOPP will be applied within Information Operations (IO) activities. This allows for an additional simplification and application of the final process. Notwithstanding the reduction, there must be taken into account a certain level of implied tasks that are critical to all missions. The command staff and associated friendly forces should be familiar with these concepts through both tenure and training. That is not to say that forthright communication will not be required to ensure that all allied commanders are in agreement to the mission at hand; however, many of the fundamental concepts that are true within all mission contexts can be exclude from the plan (Figure 3). The final operational order will not convey every single aspect of what can or cannot be performed in the mission, as these concepts should already be understood (Table 5). Essential tasks are tasks that must be addressed within the communication in order for the mission to succeed. These tasks are included in the planning and documentation process to ensure the proper dissemination of responsibilities. These concepts will be included and addressed in further detail in the mission statement.[49]

[49] *Joint Information Operations Planning Handbook.* Joint Forces Staff College Joint Command, Control and Information Operations School. (September 2009), IV-149-150.

| Joint Operation Planning Process (JOPP) |
|---|
| Step 1: Initiation |
| Step 2: Mission Analysis |
| Step 3: Course of Action (COA) Development |
| Step 4: COA Analysis and Wargaming |
| Step 5: COA Comparison |
| Step 6: COA Selection and Approval |
| Step 7: Plan or Order Development |

Table 5. The Joint Operation Planning Process [50]

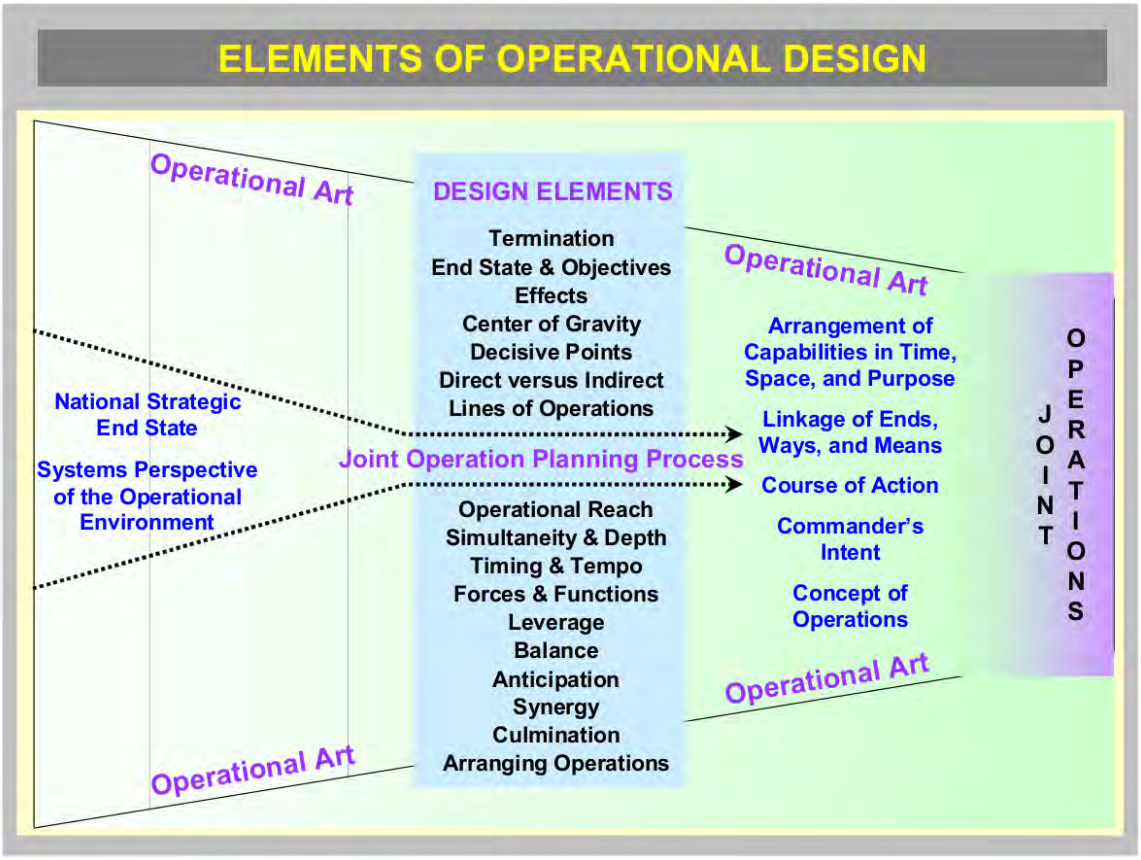



Figure 3. Elements of Operational Design[51]

[50] *Joint Operation Planning: Joint Publication 5-0.* (26 December 2006), *III-20.*

[51] *Joint Operation Planning: Joint Publication 5-0.* (26 December 2006), IV-5.

### 1. Step One: Initiation

The JOPP begins with the initiation step. The process is set into motion in response to a real or perceived threat by an authority assigned responsibility to engage military support. In some cases, the threat may not have an active adversarial threat agent, but the probability of the threat agent materializing to drive the threat is highly probable in the future. The threat may also possess only a moderate probably, but the impact of an adversarial force taking this course of action would be catastrophic. In any case, the process is created in response to a request by the hierarchy over the commander to address a perceived need. It is important to note that the Initiation and Mission Analysis steps may be combined in some situations, as well as the COA Comparison and Approval.

### 2. Step Two: Mission Analysis

Mission analysis conveys the purpose, actions, and reasoning regarding the situation that brought about the initiation of the planning process. This involves the adversarial Centers of Gravity (COG) and the corresponding events that have led to this action. The situation that led to the decision for initiation of the JOPP and the mission details are outlined and disseminated to the concerned parties. This will include enough information to build sufficient situational awareness regarding known facts, upcoming tasks, operational limitations, the desired end state, risk assessments, and initial staffing estimates (Table 6). The mission statement will capture the goal of the operation with the commander's initial intent.

| Mission Analysis Sub-Steps |
|---|
| Determine known facts, current status, or conditions |
| Analyze the higher commander's mission and intent |
| Determine own specified, implied, and essential tasks |
| Determine operational limitations |
| Develop assumptions |
| Determine own military end state, objectives, and initial effects |
| Determine own & enemy's center(s) of gravity and critical factors |
| Determine initial commander's critical information requirements |
| Review strategic communication guidance (when applicable) |
| Conduct initial force structure analysis |
| Conduct initial risk assessment |
| Develop mission statement |
| Develop mission analysis brief |
| Prepare initial staff estimates |
| Publish commander's planning guidance and initial intent |
| **Simplified Sub-Steps** |
| 1) What is the current state?<br>Determine the current state |
| 2) What is the desired state?<br>Interpret the mission, intent, and desired end state |
| 3) How will the desired state be achieved?<br>• Identify enemy COGs<br>• Develop objectives (MOEs and MOPs)<br>• Conduct initial force structure analysis<br>• Conduct initial risk assessment<br>• Prepare initial staff estimate<br>• Create mission statement |

Table 6. Mission Analysis Sub-Steps[52] [53] (Steps Not Necessarily Sequential)

[52] *Joint Operation Planning: Joint Publication 5-0*. (26 December 2006), III-21.

[53] *Joint Operation Planning: Joint Publication 5-0.* (26 December 2006), IV-5.

### *a. Center of Gravity (COG)*

Possibly, the most important aspect of Mission Analysis is the determination of allied and enemy Centers of Gravity (COG). The enemy's center of gravity is "the source of power that provides moral or physical strength, freedom of action or will to act."[54] An adversary's COG is usually described by the intelligence units assigned to conduct the investigation. The importance of establishing the adversarial, and friendly COGs lies within the hierarchy of Critical Capabilities (CC), Critical Requirements (CR), and Critical Vulnerabilities (CV) from which the objectives that will both protect allied force COGs and destroy enemy COGs will be created (Figure 4). Critical capabilities are the physical, cognitive, or informational assets that enable an adversarial or allied force to achieve their COG. Critical requirements are the conditions that must exist for the critical capabilities to operate effectively. Critical vulnerabilities involve aspects of the CRs that are exposed to attack.

[54] Joint Operation Planning: Joint Publication 5-0. (26 December 2006).

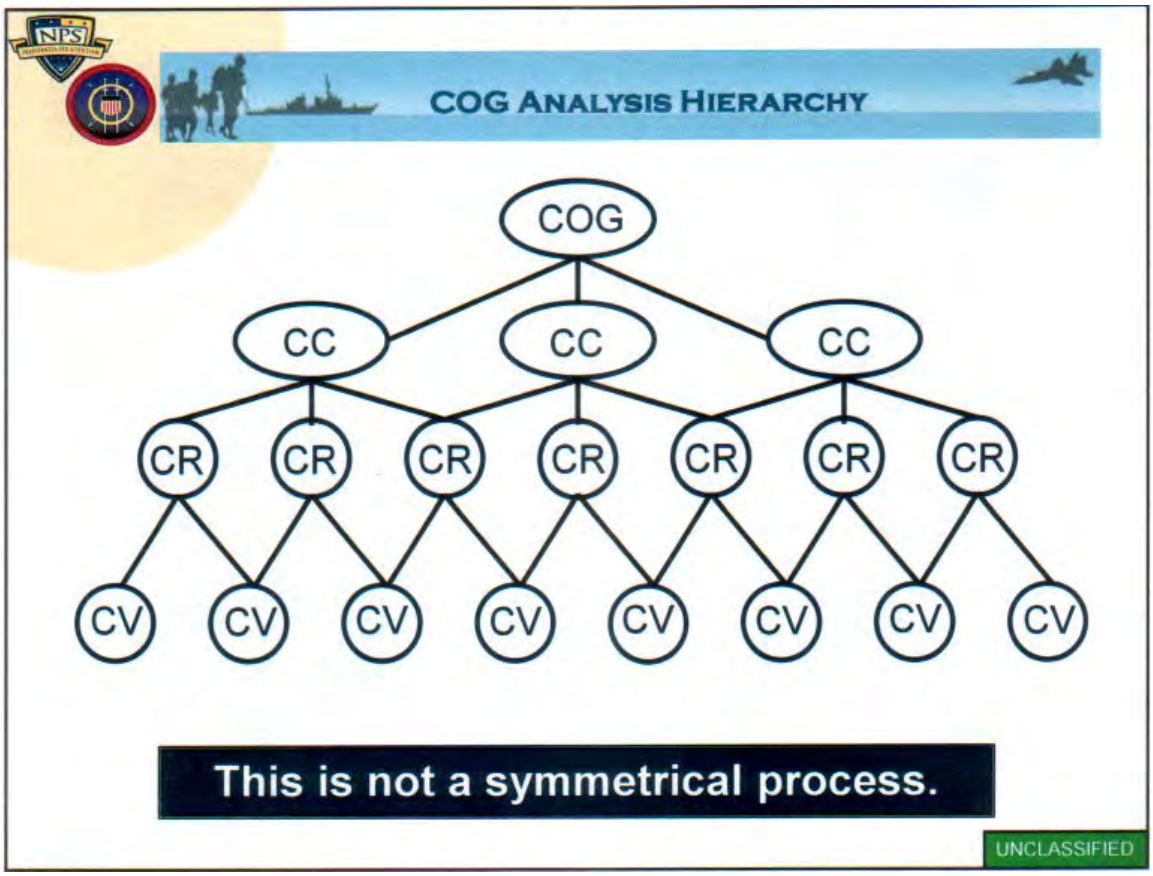


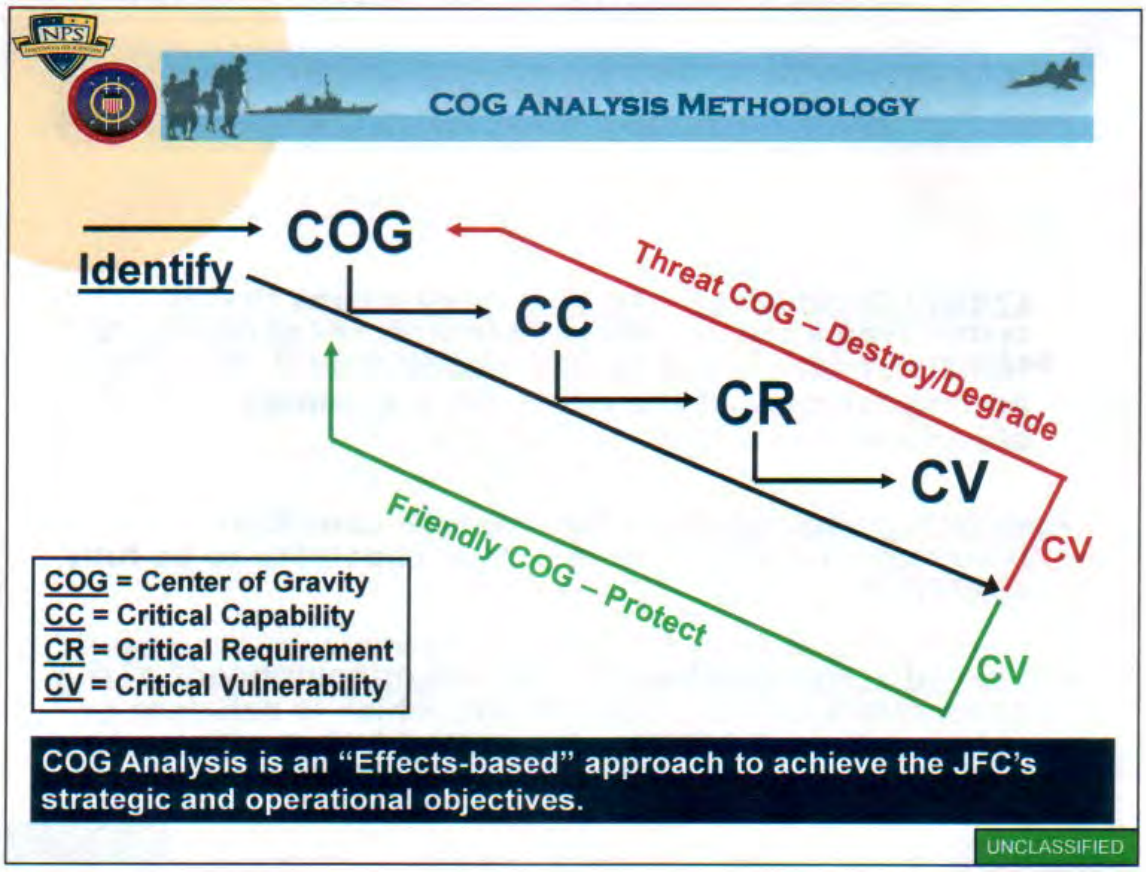

Figure 4. COG Analysis Hierarchy[55]

The proper determination of both the allied and adversarial COGs are critical to the effective planning of attack and protection measures. A poorly planned operation will not adequately identify COGs, causing the improper allocation of force resources to ineffective means. The improper allocation of military, economic, diplomatic, or psychological force will lead to unnecessary expenditures and an increased loss of life. This is not to say that planning will be complete. There will be missing bits of information for which the planner will need to make assumptions. The assumptions, if not properly validated, become risks.

[55] Edward Fisher, *Center of Gravity Analysis* (slideshow), Naval Postgraduate School, Course IO4300, 2010.

This process is taken into consideration through specified, implied, and essential tasks. Specified tasks are those objectives that have been handed down by a higher command. The implied tasks are objectives that are a dependency for the stated objective. Finally, the essential tasks are those goals that must be achieved for the mission to be a success. The essential tasks are recorded in the mission statement.

Throughout the planning process, risk analysis is conducted regarding the allied vulnerabilities, potential threats to these vulnerabilities, the likelihood of occurrence of the stated threat, and the impact of a successful adversarial exploitation of the identified vulnerabilities. Decisions will be made to mitigate, transfer, avoid, or accept the risk associated with the operation. In some cases, the risk will need to be accepted without much consideration to countermeasures. This is not the most preferred situation, but it is a requirement to maintain the agility of battle operations.




COG Analysis Methodology[56]

### *b. Mission Statement*

One of the key outputs of the Mission Analysis step is creation of a mission statement, the initial planning guidance, and Critical Commander's Intelligence Requirements (CCIR). A good mission statement covers five key questions regarding the mission: who, what, when, where, and why. This is to the exclusion of the "how" question. The method by which the mission will be conducted to specifically achieve the desired end state is not discussed within the mission statement. The statement should include a rough estimate of staffing and planning for a generally expected Course of Action (COA). This will include a discussion of the enemy Centers of Gravity (COG)

56 Joint Pub 5-00.1, *Joint Doctrine for Campaign Planning*, ll-6 and ll-11; http://www.dtic.mil/doctorine/jel/doddict/index.html; Centers of Gravity and Critical Vulnerabilities by Dr. Joe Strange (Marine Corps University Foundation, Quantico, Virginia, 1996).

and the timing in which the operation should be conducted. Additional reference to the Rules of Engagement (ROE) and the Laws of Armed Conflict (LOAC) will also be covered to an acceptable level of detail.

From an operational standpoint, there are three questions that must be answered: 1) What is the current state?, 2) What is the desired state?, and 3) How will the desired state be achieved? These questions frame the entirety of the mission in a form that can be easily conveyed to personnel situated in any location. Communicating a simple statement answering each of these questions will allow the intent and process to be delivered in an understandable format that will facilitate more expedient comprehension of the mission to be accomplished.

### 3. Step Three: Course of Action (COA) Development

The most important step within the JOPP is the development of the COA. Generally, three COAs will be developed, including contingency actions which address unexpected or alternative situations. At this point of the process, the process will address the specific circumstances surrounding the who, what, when, where, why and how questions detailing how the mission will be conducted. The first three courses of action will offer alternative viewpoints on how the mission could be accomplished. This must include the actions, concepts, time estimates, and success criteria. The objectives, effects, actions, resources, and risks are thoroughly discussed and documented within the process. They must be performed within with respect to the "restraints," activities that must not be conducted, and the "constraints," activities that must be conducted for the success of the mission. There are numerous opportunities that may arise that will not be available for action due to the restraints surrounding the operational environment. The general concepts and specific actions should be documented and communicated appropriately, according to the level of acceptable risk. After thoughtful design, COAs are presented to the commander for approval and escalation to analysis and wargaming (Table 7).

| Valid Course of Action |
| --- |
| **Adequate** — Can accomplish the mission within the commander's guidance. |
| **Feasible** — Can accomplish the mission within the established time, space, and resource limitations. |
| **Acceptable** — Must balance cost and risk with the advantage gained. |
| **Distinguishable** — Must be sufficiently different from the other courses of action. |
| **Complete** — Must incorporate:<br>• objectives, effects, and tasks to be performed<br>• major forces required<br>• concepts for deployment, employment, and sustainment<br>• time estimates for achieving objectives<br>• military end state and mission success criteria |

Table 7. Valid Course of Action[57]

It is important to note that within the context of information operations planning as integrated into the joint operation planning process, there is significant discussion about the effect that the process will incur on the physical, cognitive, and informational spheres. The action-reaction model allows for forces to plan their own operations, while being mindful of adversarial actions. The goal is to establish an understanding of how and when information must flow within the battle space in order for allied and enemy commanders to make educated decisions. The circular process begins within the physical realm with the action itself. The action is relayed to the information realm where data are collected, processed, and disseminated. Afterwards, it enters the cognitive phase where situational awareness and decision-making take place. This brings the forces back into the information realm where the data are processed and then disseminated. The process ends with the next action that the force will make relevant to the changes in the battle space (Figure 5).

[57] *Joint Operation Planning: Joint Publication 5-0*. (26 December 2006), III-28.

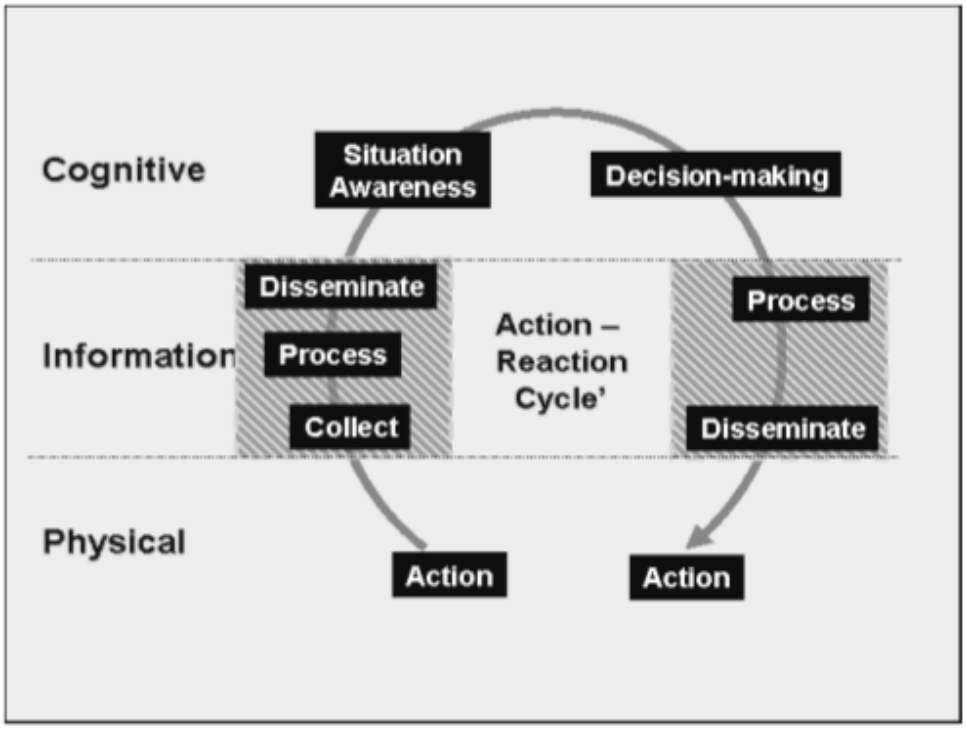



Figure 5. Action-Reaction Model[58]

IO integration into JOPP also allows for a more specific view of COA development in relation to the specific steps that should be taken to achieve a set of goals. The process is augmented to include objectives, effects, and tasks. Objectives are allied goals required to achieve the mission's end state. Effects describe what type of behavior should be exhibited within the battle space. Tasks are the specific actions that are taken to generate the effects to meet the objectives.

Mission → Objectives → Effects → Tasks

"IO EFFECT = TARGET + IMPACT ON A SYSTEM OR BEHAVIOR" [59]

The generation of IO Effects within the mission scope involves the "What," "Who," "Why" of the objective. The "How" concept is addressed during the

[58] *Joint Information Operations Planning Handbook.* Joint Forces Staff College Joint Command, Control and Information Operations School. (September 2009), IV-169.

[59] *Joint Information Operations Planning Handbook.* Joint Forces Staff College Joint Command, Control and Information Operations School, September 2009, IV-173.

development of the IO Tasks.[60] Successful IO Effect determination requires a clear understanding of what is to be accomplished, how it will be measured, and the synchronization of forces that will make it happen (Table 8). The incorporation of multiple forces to accomplish a single stated goal can be better facilitated through this process when the plan is created with the outcome in mind.

The force tasked with creating the desired IO Effect should understand Measures of Performance (MOP) versus Measures of Effectiveness (MOE). MOP is the completion of a subset of tasks that must be accomplished within the scope of ordinary work. A MOP for the distribution of leaflets over a foreign city could be relevant to the number of leaflets dropped in a certain time period, the number of jams that occurred in the distribution system, the quantity of personnel that were required to conduct the operation, etcetera. The MOP does not indicate that the desired IO Effect was generated. There is no indication that the targeted population changed a behavioral pattern, such as surrendering, in the light of the measurement provided to the command. A report of 100,000 leaflets demanding surrender of the adversarial forces that were dropped over a thousand square miles of enemy territory does not convey the success or failure of the IO Effect. This does indicate that the forces were successful in conducting their job as expected without significant impedance.

To convey the accomplishment of a desired outcome requires the clear communication of the final objective and the MOE. The MOE relates the process that was conducted and the result. One hundred thousand leaflets demanding surrender of adversarial forces that were dropped, and 48 percent of the forces surrendered is an example of a MOE. In this case, the effect of the dropped leaflets on the targeted population is reported. This allows the commander to adjust the specifics of the operation to better achieve the desired effect. In this case, the commander must be made aware of the MOP that the leaflets were successfully dropped, and also the MOE, that the message on the leaflets had the intended effect. If the forces had failed to drop the prescribed number of leaflets over the target area, the MOE may have been affected by

[60] Edward Fisher. IO4300, July 2010.

the lack of leaflets or the message. It would be unknown if the failure was related to the unsuccessful task or if the message on the leaflet was ineffective.

| **The proper development of IO Tasks involves the following steps** |
|---|
| Step 1) Select the target<br>• Center of Gravity<br>• Commander's Objective<br>• Cognitive Dimension<br>• Information Dimension<br>• Physical Dimension |
| Step 2) Determine the desired action that will make the appropriate physical or behavioral change<br>• Destroy<br>• Disrupt<br>• Degrade<br>• Deny<br>• Deceive<br>• Exploit<br>• Influence<br>• Protect<br>• Detect<br>• Restore<br>• Respond |
| Step 3) Relate the purpose of the action to the desired outcome |
| Step 4) Assign a resource to complete the task |

Table 8. IO Tasks

### 4. Step Four: COA Analysis and Wargaming

COA analysis and wargaming takes the proposed courses of action and places them into a battle scenario. Each plan is tested by the allied forces who assume roles as an enemy "red cell" or an allied "blue cell." This allows the forces to conduct a simulated battle using actual command decisions and retaliation. The simulation will expose weaknesses in allied force actions as the enemy force retaliates. Creative responses to the simulated enemy retaliations can be incorporated into additional mission

capabilities or used to adjust or create new COAs, as desired. For more information, the IO Cell Actions and Outcomes as part of Joint Planning Packet appears in Appendix A.

The staff follows nine steps during the wargaming process:[61]

- Organize for the War game.
- List all friendly forces.
- List and review enemy forces, ECOAs, and outstanding RFIs.
- Review assumptions.
- List known critical events.
- Determine Governing Factors.
- Select the war game method.
- Record and display results.
- War game the operation and assess the results.

### 5. Step Five: COA Comparison

The comparison step of the process places the COAs against the final mission objective, not one another. COAs are not compared with other COAs, but the outcome of the wargaming and analysis of each COA to achieve the end state is considered. The desire is to find the COA that minimizes risk, allows for future operations, has the maximum flexibility and agility for addressing unexpected threats and opportunities, and pushes the ability for individual initiative to subordinates whenever possible. Subordinate commands should have the ability to take personal initiative to accomplish the stated goals and exploit new opportunities whenever possible. This allows for the continued development of the leadership and forces, and the ability to take advantage of unexpected opportunities that may arise within the battle space.

### 6. Step Six: COA Selection and Approval

The course of action selected for submission to the higher command is relevant to the interpretation of the analysis and comparison results by the subordinate command.

61 *Joint Operation Planning Process (JOPP) Workbook.* NWC 4111H. (JMO Department, Naval War College, 21 January 2008), 3-3.

The staff may use a decision matrix or other selection criteria, but the final decision will be based on the conscious decision by the commander in regards to the ability to accomplish the goal with the stated COA. This process may involve the selection of more than one COA to the higher command, in order to either compensate for expected changes in the battle space, or to provide an alternate plan based on the commander's personal estimate, experience, and judgment (Figure 6).

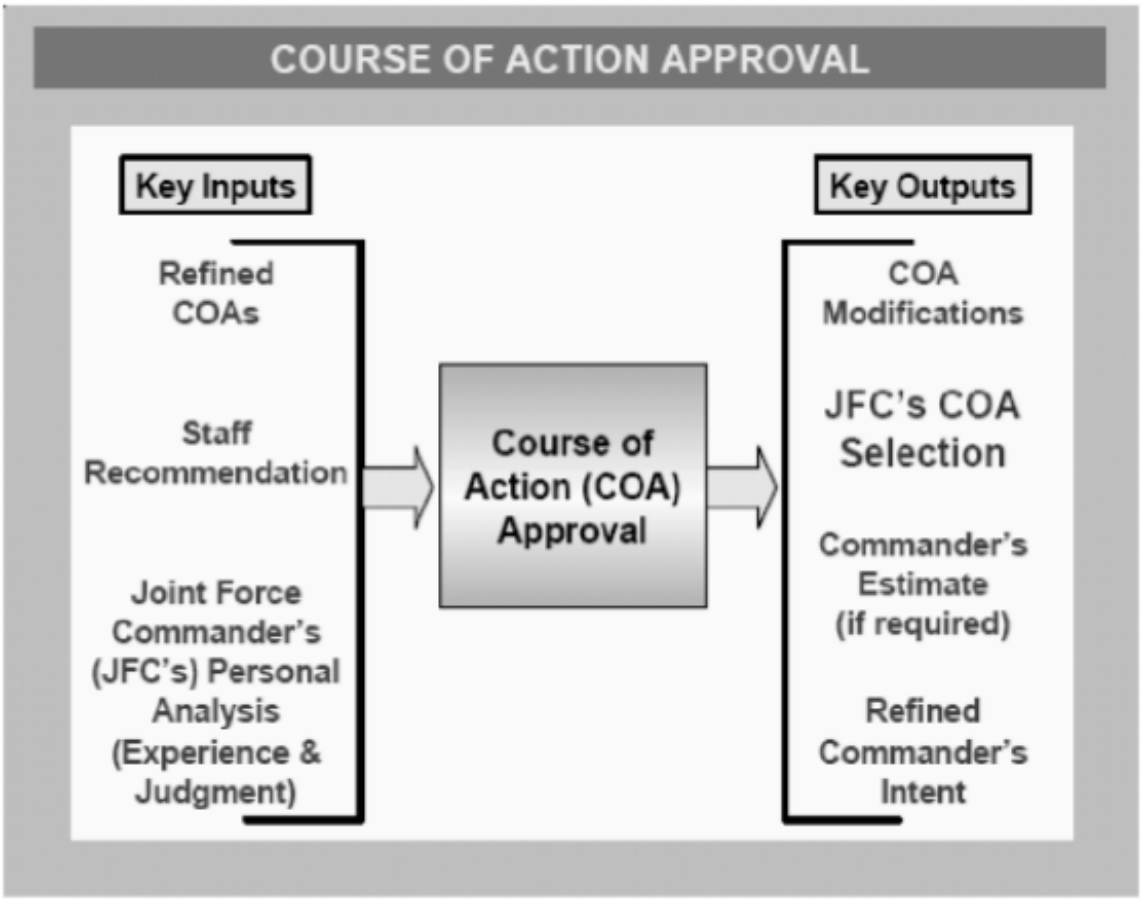



Figure 6. Course of Action Approval[62]

62 *Joint Operation Planning: Joint Publication 5-0.* (26 December 2006), III-30.

### 7. Step Seven: Plan or Order Development

The final step is the creation of a plan or order that will be communicate to subordinate and collaborating organizations and components. The subject matter experts will be acquired to accomplish the IO objective creation and task orders.

## C. CONCLUSION

The JOPP allows for the comprehensive creation and evaluation of actions to meet the operational objectives. The coordination and collaboration with allied commands and related components is improved through the increased synchronization that is achieved through following the JOPP. Information Operations concepts augment this process to the extent that it may be correlated to enterprise security planning. As the allied and adversarial centers of gravity become more pronounced through the process, the capabilities on which they rely can be more easily identified. As in enterprise security planning, this allows for the exposure of the critical requirements and associated vulnerabilities. The JOPP, in its many variations, provides an excellent planning framework to achieve both military and civilian operational objectives.

THIS PAGE INTENTIONALLY LEFT BLANK

# IV. ENTERPRISE INFORMATION SECURITY FRAMEWORK DEVELOPMENT

It is not uncommon for the implementation of a thorough security framework such as CobiT or the ISO 27001 to take years of planning and design.[63] Enterprise security should have a process that allows a management team to address the critical vulnerabilities affecting the firm's centers of gravity both rapidly and effectively. It is currently reported that over 100,000 new websites are discovered that harbor viruses every day.[64] The threat landscape surrounding organizations can change far too rapidly for such delays to be acceptable within the information security industry. The changes that can take place in as little as eighteen months can bring about a complete paradigm shift of how business and regulatory compliance is accomplished. Remote web access, tablet computers, smart-phones, smart-vehicles, usb-powered computers, and other systems present new capabilities and threats to corporate viability. Possessing a framework that allows for the flexibility to utilize existing management systems, the agility to address emerging threats, and the speed required to provide adequate protection against new threats is required.

The development of a framework that takes into account the many varied aspects of business acumen, as well as, the expert skill of a security professional is one of the primary outputs that can be initiated after thorough study of the public and private industrial planning processes and frameworks. In the following section, discussion will center around the key components of the JOPP as interpreted for the needs of enterprise security. Offensive measures are relegated to the legal statutes already in place within the country that exercises malicious intent against the corporate assets. Many methodologies have approached these tasks with overwhelming complexity. One of the

63 Charles Robb, "Desperately Seeking Security Frameworks – A Roadmap for State CIOs," NASCIO. March 2009, Accessed July 17 2011. http://www.nascio.org/publications/documents/NASCIO-SecurityFrameworks.pdf.

64 "Cyveillance testing finds AV vendors detect on average less than 19% of malware attacks," 4 August 2010, http://www.cyveillance.com/web/news/press_rel/2010/2010-08-04.asp (accessed 17 August 2011).

primary goals of implementing the JOPP into enterprise security planning is to reduce complexity, providing a straightforward process that will define and address the most important objectives to the firm.

## A. OVERVIEW

Enterprise security planning must be seen more in the context of a battlefield than in that of a business. Business systems are created within fixed laws, rules, and regulations. There are expected codes of conduct and prudent judgment that can be relied upon for decisions. There are situations within the business world where both sides can come to a mutually beneficial agreement. Business is about the provision of services to those that wish to possess them in a way that benefits both parties. This is in contrast to war or conflict, in which one nation or actor threatens or displays aggressive actions to another. The enemy may attack outside of regular business hours, using channels outside of normal business operations. To damage the sales revenue of a product line, the enemy may attack the support staff or knock out the electricity surrounding the service providers. False statements may flood the Internet and media regarding product or service failures. The development of an information security program that is capable of supporting business operations while disrupting adversarial attempts to damage the firm's revenue falls outside of the scope of business as usual. Information security is more battlefield than business, and the objectives therein must be conducted as such.

> In forming the plan of a campaign, it is requisite to foresee everything the enemy may do, and to be prepared with the necessary means to counteract it. Plans of campaign may be modified, ad infinitum, according to circumstances; the genius of the general, the character of the troops, and the topography of the theater of action.[65]

The JOPP can be used for general enterprise security development, as well as, targeted employment of systems to mitigate specific threats. In the most general application, the JOPP provides guidance for Strategic Direction (Business Strategy), Force Structure (Staffing), and Command and Control (Strategic Communications). The

[65] Napoleon. *Napoleon's Maxims of War: Maxim II* (1831).

military already has established a rigid organizational hierarchy and culture. Corporations must establish the mission, staffing, and method of garnering support through communications in order to meet their operational and production goals. In this preliminary phase, a corporate entity would ask three basic questions: 1) What is the current state?, What is the desired state?, and How will the firm achieve the desired state? In these questions, the firm's strategy, staffing, communications, and production goals are reviewed and discussed in relation to the market limitations and associated risks. Enterprise security planning will take place within the context of an already established firm, integrating into the business operations in the most transparent way possible.

The key to operational design essentially involves (1) understanding the strategic guidance (determining the end state and objectives); (2) identifying the adversary, principal strengths and weaknesses; and (3) developing an operational concept that will achieve strategic and operational objectives.[66]

It is the goal of a good information security program to maintain invisibility to internal and external operations, except when it intends to coerce action through its own visibility. When information security programs choose to be visible, it should most often be in the role of a deterrent, not in the prevention, detection, or response roles. The prevention, detection, and response operations should be quietly accomplished with minimal impact to the firm's public or private image. If a response to an attack is acknowledged publicly or within the organization's own network, it should be disseminated through a strategic communication that will be used to accomplish the desired deterrent effect.

## B. JOPP: PLANNING FUNCTIONS

To develop a good enterprise information security program, many of the steps outlined within the JOPP can be effectively used. These steps can be interpreted into phases aimed at achieving a specific goal. Earlier, the general aspects of the JOPP were interpreted for general business use. At this point, the specific steps relevant to enterprise security planning will be detailed using both the overall JOPP strategic function and the

66 *Joint Operation Planning: Joint Publication 5-0.* (26 December 2006), xvii.

specific JOPP steps. This chart correlates the requirements for enterprise security relative to the overall JOPP planning functions (see Table 9).

| JOPP: Planning Functions | Enterprise Security: Planning Functions |
|---|---|
| 1. Strategic Guidance. | 1. Strategic Alignment. |
| 2. Concept Development. | 2. Risk Management. |
| 3. Plan Development. | 3. Concept Development. |
| 4. Plan Assessment (Refine, Adapt, Terminate, Execute). | 4. Senior Management Communication and Advocacy. |
| | 5. Policy Development. |

Table 9. JOPP: Planning Functions[67] and Enterprise Security Planning Functions

As can be seen within the chart, the JOPP provides similar strategic functions to those that would be needed within any enterprise security governance program. These steps bear some resemblance to concepts common within project management or general enterprise governance. The importance of these similarities are not fully realized within the general JOPP planning functions, but within the specific steps. In this case, the JOPP planning functions provide a foundational understanding illustrating the complete integration into the Joint Operation Planning Process. There is not a complete correlation between the two concepts, but the similarities are of great use to further planning.

The enterprise security planning functions deviate from the standard JOPP in strategic alignment, risk management, and communication. Within the corporate environment, security management is not the core purpose of the business. Even within the security industry itself, security firms do not have a primary mission of becoming secure and maintaining security. The corporation's primary mission is to provide a product or service. This product or service may be for profit or entirely free, as in a philanthropic endeavor; nonetheless, the mission is to produce some solution for some market. Therefore, the "Strategic Guidance" aspect of the JOPP is replaced with

67 *Joint Operation Planning: Joint Publication 5-0*. (26 December 2006), I-15 to I-16.

"Strategic Alignment." This is because the firm already exists with a purpose other than being secure, and the enterprise security function must provide protection for the production of a product or service.

In the military environment, communication channels are more strictly defined and are often delegated to a communication officer or conducted within a formal process. The corporate design requires a more simplistic model that provides for open communications between the security officer and the senior management representatives. In this case, the security officer notifies the higher command echelons of the need to initiate a formal plan in response to a risk analysis. The risk assessment is conducted with only a cursory analysis of the firm's assets and centers of gravity. An in-depth analysis will be conducted within the formal planning process. At this point, the senior management team must then be persuaded that the mission objectives are within the best interests of the firm. Once the security officer has approval to engage in the requisite planning process, policies are developed for the firm. This process deviates slightly from the concept development portion of the JOPP to include risk management as a prerequisite. This is required, as the security officer will be responsible for both the initiation, development, and policies to mitigate risks, as well as, persuading the firm to invest the resources required for the program.

## C. ENTERPRISE SECURITY USING THE JOPP

The overall planning process developed in this research entitled, Enterprise Security Planning Process (ESPP) is adjusted to meet the more confined needs of a corporate security environment. For instance, "Step 1: Initiation" will be interpreted as part of the strategic guidance within the organizational needs of the firm and will be combined with portions of "Step 2." "Step 2: Mission Analysis" will be reduced and subdivided into multiple aspects of both the organizational and departmental goals. There will also be a combination of the individual COA development, analysis, comparison steps, into one phase. Each of the steps will be evaluated based on the urgency and importance of the action. "Step 6: COA Approval" will be restated to

"Program Approval and Budgeting," leaving "Step 7: Plan or Order Development" to be interpreted as an implementation and acquisition phase.

This modifies the JOPP to a new form providing for the following phases: Initiation, Program Analysis, Planning, Approval and Budgeting, Acquisition and Implementation, and Auditing and Revision. Providing this simple framework allows for a reduction in the complexity often experienced when addressing enterprise security while leveraging the maturity of the JOPP. The actual policies and procedures involved in securing the firm involve much greater detail and varied levels of expertise for implementation. The Joint Operation Planning Process and the Enterprise Security Planning Process are presented in the included chart (see Table 10).

| Joint Operation Planning Process (JOPP) | Enterprise Security Planning Process (ESPP) |
|---|---|
| Step 1: Initiation | Phase 1: Initiation |
| Step 2: Mission Analysis | Phase 2: Program Analysis |
| Step 3: COA Development | Phase 3: Planning |
| Step 4: COA Analysis and Wargaming | Phase 4: Approval and Budgeting |
| Step 5: COA Comparison | Phase 5: Acquisition and Implementation |
| Step 6: COA Selection and Approval | Phase 6: Auditing and Revision |
| Step 7: Plan or Order Development | |

Table 10. JOPP[68] and ESPP

### 1. Phase One: Initiation

The JOPP provides for an initiation step that is the result of an actual or perceived threat against a national interest. Initiation, as seen in the JOPP, is the result of a formal process delegated by a higher command. Enterprise security departments are faced with continual threats from multiple agents on an ongoing basis. The purpose of the department is to protect the firm's assets from unauthorized disclosure, alteration, or destruction. These units are concerned with providing confidentiality, integrity, and availability of firm resources at all times, recommending the initiation of protective

[68] *Joint Operation Planning: Joint Publication 5-0*. (26 December 2006), III-20.

controls as the result of a self-imposed audit, external audit, incident, or regulation. In most, if not all, of the cases mentioned, the enterprise security unit initiates the process. As such, there is a deviation from the standard interpretation of the JOPP's initiation to relegate the initiation from within enterprise security itself.

In the preliminary portion of the Initiation Phase, alignment must be achieved with the core purposes of the organization. Within this context, strategic communications are planned to convey the purpose of the initiative and continually reinforce the organizational mission. Strategic communications vary from normal daily discussions in the following ways. First, strategic communications are defined by scope. This can mean that the communications are conducted intentionally through micro, mezzo, or macro social contexts or simply by the generality or specificity of the message. These contexts can remain within the firm or they may involve a small segment of customers, all customers, or the entire public. Next, strategic communications are developed with short-term and long-term objectives in mind. These objectives take into account the message and the desired outcome. If the message was to provide immediate attention to a well-known security risk facing the firm, then a short-term impact would be expected within the organization as employees take the appropriate measures detailed within the communiqué. If the communication's goal is to alter the public perception regarding the negative environmental impact of a new competitor's product line, then the communications would require additional measures of performance to be defined to gauge the staff's workload and adequate measures of effectiveness to gauge the impact of the message itself.

The next task within the initiation phase is to properly identify roles and responsibilities within the department and enterprise. There must be a clear definition of both who is responsible for each security task and what that responsibility entails. Security awareness, planning, incident response, corporate continuity, disaster recovery, and other responsibilities are often neglected due to a failure to properly define and assign the responsibility appropriately. This is especially important during the initiation phase of the process to allow for a solid mission to be defined.

Throughout the initiation phase, the policies created within the foundational base planning functions of the enterprise security program should be reviewed for direction and propriety. Many of the policies may have been changed since the program was last initiated, causing a lack within the references to adequate controls and processes. This can lead to the creation of new policies, the revision of old policies, or the acquisition of additional details that may have been missed during the initiation.

Most of the objectives taken in response to either a potential threat or in response to an actual threat to firm operations are proposed by the enterprise security office itself. In the case of prevention, the security planning process follows the JOPP in a more controlled fashion, allowing for a more thorough and tested solution. In the event of an actual threat, the process is more similar to JOPP crisis action planning. In both cases, the JOPP provides a process that can be followed in varied levels of detail. Most often, a plan or process will already exist to manage the crisis as it is encountered simply due to the experiences of the security officer. In some cases, a new threat will take action against an unplanned vulnerability and will require a more dedicated and detailed response plan to be immediately developed.

Example Objectives:

- Security Awareness
- Identification and Removal of Critical Vulnerabilities
- System Hardening (removal of unused services, installation of patches and updates)
- Regular Background Investigations
- Regulatory Compliance
- Adequate Archival Systems

### 2. Phase Two: Program Analysis

The first step in program analysis is the discovery of physical, information, and employee assets that may be negatively affected by adversarial attacks. This is a skill,

asset, and process inventory designed to allow the enterprise security office to properly define the risks posed by various threat agents internally and externally to the firm. The impact of these assets to strategic firm operations is determined to identify which assets are the most critical to the organization.

These assets will be used in conjunction with the strategic alignment to firm operations to identify the most critical assets within the organization. This is accomplished using the JOPP model's reference to centers of gravity.

#### *a. Centers of Gravity*

The application of the military context to the business context is appropriate in this case due to the adversarial situations presented to a firm's security. Threats to an enterprise are not isolated to market conditions, customer satisfaction, or the competition. In addition to regulatory codes, the enterprise security office must mitigate situations arising from individual criminal actions, concerted acts by criminal organizations, legal and civil issues surrounding foreign governments and firms, fraudulent activities funding terrorist organizations, malicious hackers, and malevolent programs. This allows the battlefield context of the JOPP to become more easily related to enterprise security functions.

The centers of gravity for an organization can be related to the firm's core competency, core purpose, organizational mission, or key product and service offerings. This is closely related to the concept of allied and adversarial COGs as defined within a battle context. The COG is composed of critical capabilities, critical requirements, and the related critical vulnerabilities affecting them. An example of this situation is illustrated with the text and figure contained within this section (Table 11 and Figure 7).

| Example COG Analysis |
| --- |
| |
| COG = Provide Expert Investment Advice |
| |
| CC = Highly Skilled Advisors<br>CC = Fast and Reliable Technology<br>CC = Efficient Business Process |
| |
| CR = Personnel: Management<br>CR = Personnel: Advisors<br>CR = Personnel: Support Staff<br>CR = Personnel: Technical Staff |
| |
| CR = Technology: Workstations<br>CR = Technology: Servers<br>CR = Technology: Internet<br>CR = Technology: Network<br>CR = Technology: Software<br>CR = Technology: Production Data<br>CR = Technology: Sensitive Data |
| |
| CV = Personnel: Physical Unavailability<br>CV = Personnel: Physical, Psychological, or Emotional Incapacitation<br>CV = Technology: Unauthorized Disclosure<br>CV = Technology: Unauthorized Alteration<br>CV = Technology: Unauthorized Destruction<br>CV = Technology: Performance Disruption |

Table 11. Example COG Analysis

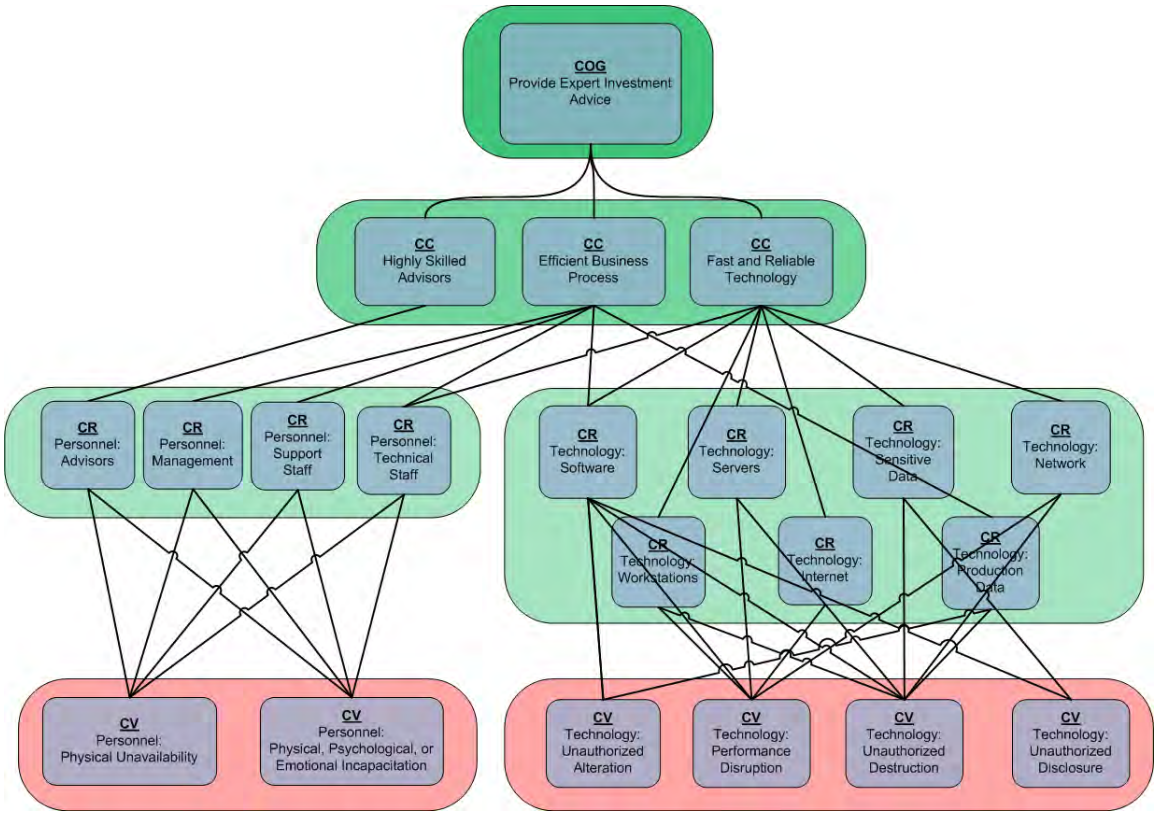



Figure 7. Center of Gravity

### *b. Risk Assessment*

The risk assessment becomes much more effective when used within the context of a proper analysis of the organization's centers of gravity. The organization's COGs allow for a quick determination of the risks facing each facet of the firm's primary functions. Without a COG analysis the strategic alignment is measured against prevalent threats facing the firm. These threats are then measured against the firm's individual productivity in an ad-hoc or formally defined expository manner. After conducting even a rudimentary COG analysis, the vulnerabilities to actual firm operations can be far more understood.

Risk assessments are part of the fundamental function of an enterprise security office.[69] The allocation of proper preventive measures will usually be determined by a formal quantitative or qualitative risk assessment process. If a quantitative risk analysis is possible, then a dollar-for-dollar comparison of the cost of an attack against the cost of prevention measures is taken into consideration. This takes into consideration the Single-Loss Expectancy (SLE), Annual Loss Expectancy (ALE), and the Annual Rate of Occurrence (ARO).[70] If the financial impact of the materialization of a threat is considered to be more than the cost to protect the systems against the threat, then the preventive solution is employed. If the financial implications for implementing the protection mechanisms outweigh the cost of a threat action, then the risk is accepted. This calculation must take into consideration the full projected cost of the protection mechanism, depreciation of the mechanism, and the annualized cost of an attack materializing against a known exposure. It is rarely possible to predict the public backlash created by an attack. The opportunity costs and relevant costs of the attack will impact more aspects of firm operations than can be easily identified. This makes the quantitative a popular theoretical approach to enterprise security management, but rarely does it meet the expectations of reality.

Having attempted to gain a quantitative risk analysis for the firm's operations with little success, most organizations will turn to a qualitative analysis method. This method allows the ascription of a value of any number, one through five, for example, to the likelihood of a realized threat with a similar assignment for the impact to firm operations in relation to the cost of prevention mechanisms.

---

69 Douglas J Landoll, *The Security Risk Assessment Handbook: A Complete Guide for Performing Security Risk Assessments* (New York, New York: Auerbach Publications, 2006), 11.

70 Ronald L. Krutz and Russell Dean Vines, *The CISSP Prep Guide: Gold Edition (*Indianapolis, Indiana: Wiley Publishing, 2003), 18.

**Non-JOPP Example:**

Incident:

SPAM. Without preventive measures, it is expected that the firm will receive 180,000 to 250,000 SPAM messages per day. This equates to roughly 150-200 messages per day for each user account.

Key:

Threat Expectancy:

1 = Unlikely
5 = Almost Certain

Impact if Ignored

1 = Unnoticed
5 = Catastrophic

Assessment:

Threat Expectancy = 5
Impact if Ignored = 3
Cost of Prevention = 1

Proposal:

Due to the negligible cost of the prevention mechanism in relation to the extreme likelihood of the occurrence of the attack in combination with the detrimental impact to firm operations, it is recommended that this preventive mechanism is implemented.

### *c. JOPP Benefit to Risk Assessment*

This process can be more clearly defined using the centers of gravity to understand the actual impact to firm operations. In the case of SPAM, an impact will be felt to the aforementioned core mission of "providing expert investment advice." It can be seen from the COG analysis that SPAM is a threat facing a performance vulnerability. The performance vulnerability will, in this case, affect the servers. This affects the fast and reliable technology capability, resulting in a failure to provide timely investment advice. The straightforward approach outlined in the JOPP through use of the COG analysis and development will allow the security office to better communicate the

importance of the threat to the senior management, more easily gain funding, and more directly protect against an adversarial process affecting the core mission of the firm.

### 3. Phase Three: Planning

The planning phase involves the research of potential solutions, the development of appropriate courses of action, and the construction of a timetable for the communication and implementation portions of the Enterprise Security Planning Process (ESPP). The investigation surrounding possible solutions within the technical environment is quite daunting. Technical capabilities are doubling faster than every eighteen months. This rapidly changing environment requires that the architect tasked with discovering viable solutions to meet the mission objectives must be continuously observing the market and gaining new skills.

The proper determination of a course of action, as referenced in the previous chapter, involves the distinct definition of a feasible action plan that can be completed within a defined time frame using a predetermined amount of force. During the planning phase, the teams involved will need to conduct normal project management tasks to overcome fundamental challenges. The project plans take place at a more detailed level than the ESPP, as such, the personnel involved will need to possess adequate skills, budget, time, and authority to affect the required changes.

Communications are the fundamental building block of personal advocacy within, and outside, an organization. Communications should be scheduled within the ESPP to notify the concerned parties of the initiation, timetable, progress, and complications during the execution of the initiative. The type of communication should be crafted within the strategic purpose of the initiative and firm to allow feedback to occur. Feedback and attention to individual needs and desires will help prevent the backlash that can occur when personnel or teams resist a program. The importance of friendly and persuasive language, framed in a strategic context, cannot be overemphasized. Neglecting the personal opinions of the affected parties will lead to inefficiencies and possibly even downright insubordination. Proper communication will disarm the disgruntled personnel and encourage the involved staff to complete the task at hand.

Finally, the implementation should be scheduled with respect to the risk, cost, and personal interests of those involved. This prevents an implementation from absorbing a twelve-hour workday during Christmas holidays, while paying twice the normal labor rates, all for a solution that could have waited another three months. If key participants have personal conflicts that may affect the schedule adversely, a minor tweak in the scheduling will aid in the advocacy of those participants in the future.

### 4. Phase Four: Approval and Budgeting

The approval phase is much like the JOPP COA Analysis, Wargaming, and Comparison steps. In this phase, the courses of action are not only approved in methodology, but they must also meet budget requirements. Security operations should be conducted within short time periods, preventing exploitation from known or perceived threats as quickly and effectively as possible. This goal however, may run in contrast to recent market downturns or budgeting shortfalls. In these cases the initiative may be denied in the current state due to budgetary reasons, but not in principle. In this case, the initiative will need to be redesigned to fall within the budget limitations or the associated risks will need to be accepted until the budget is available. This decision must be shared among senior management to avoid legal or personal liability caused by the stagnation of the initiative.

### 5. Phase Five: Acquisition and Implementation

Once the program is approved and a budget is defined, the process turns to competitive quotes, shipping and training time frames, and implementation scheduling. At this point, the subject matter experts involved in each detailed aspect of the initiative will be summoned and allocated to the relevant project teams. Enterprise security initiatives often require the participation of public relations, legal, compliance, information technology, human resources, and the specific departments affected by the change. Once again, persuasive and friendly communication conducted early and often can speed the implementation and ease the internal and external backlash often associated with additional security control mechanisms or processes.

### 6. Phase Six: Auditing and Revision

After the initiative is complete, an audit will allow for a gap analysis to be conducted. The gap analysis will summarize the difference between the initiative's designed end-state and the actual end-state.[71] In most cases, this is a small difference that can be corrected through a few minor projects. In many cases, it is never formally addressed and causes inefficiency and system failure in complex environments. In any case, the acknowledgement of a few minor imperfections or urgent modifications does not indicate a mission failure.

This also includes a chance for lessons learned and revision to the systems or processes for future initiatives.[72] Enterprise security offices will have a continuous bombardment of risks to address from existing and new product or service offerings, as well as, new and existing threats. A safe and appropriate summary of the success and failure experienced during the initiative will aide in more effective and efficient initiatives in the future.

## D. CONCLUSION

The overall Enterprise Security Planning Process (ESPP) as instituted within the context of the JOPP can offer a mature and simple method by which an enterprise security office can manage operations. A more complete representation of the enterprise security planning phases, as interpreted using the JOPP, is represented in the expanded chart (Table 11). The detailed aspects contained within a normal security operation can be reviewed within the various appendices contained within this report.

---

71 Douglas J Landoll, *The Security Risk Assessment Handbook: A Complete Guide for Performing Security Risk Assessments* (New York, New York: Auerbach Publications, 2006).

72 *Joint Information Operations Planning Handbook.* Joint Forces Staff College Joint Command, Control and Information Operations School. (September 2009), IV-247-250.

| Enterprise Security Planning Process: Overview |
| --- |
| Phase 1: Initiation<br>• Strategic Alignment<br>• Strategic Communication Planning (message + response, to whom?)<br>• Define Roles and Ongoing Responsibilities<br>• Policy Assessment |
| Phase 2: Program Analysis<br>• Define critical physical assets, information assets, and personnel<br>• COG Analysis (CC, CR, CV)<br>• Risk Assessment based on Centers of Gravity |
| Phase 3: Planning<br>• Investigate available solutions<br>• Determine courses of action<br>• Schedule communications<br>• Schedule implementation |
| Phase 4: Approval and Budgeting<br>• Present potential courses of action<br>• Gain support from senior management<br>• Begin acquisition process |
| Phase 5: Acquisition and Implementation<br>• Begin communications campaign to inform and influence<br>• Procure the requisite personnel, processes, or products |
| Phase 6: Auditing and Revision<br>• Internal<br>• External<br>• Initiation for new people, processes, or systems |

Table 12. Enterprise Security Planning Process

THIS PAGE INTENTIONALLY LEFT BLANK

# V. CONCLUSION

## A. THE SITUATION

Current enterprise security planning methodologies are inadequate and inappropriate for managing the onslaught of threats facing organizations in such a rapidly changing adversarial landscape. An implementation period of greater than eighteen months is woefully inadequate to produce the agility required for a doubling of attack vectors. The concept of long-term planning within overly complex frameworks that offer solutions based on sixty to eighty percent compliance is antiquated, costly, and dangerous. Both the threat landscape and the management structure change too quickly for a plan whose goal is eighty percent compliance within a three-year period. Most frameworks will admit that no firm will be capable of a complete implementation. The plans are designed to be continuously revised from core concepts to administrative process on a regular basis. It is not viable to implement a plan to eighty percent effectiveness that will manage one hundred percent of the firm's security exposure. If this plan is then revised at the time that it achieves eighty percent effectiveness, the new level of compliance to the framework will be significantly less. Each reevaluation of the system will result in a less capable program that leaves the core competencies of organizations exposed to malicious attack. This reality has been demonstrated multiple times through data spillage that has occurred because of a failure to secure the most basic aspects of the firm's resources. The prevailing cause of these failures is the constant revision of a program that never reached full maturity during the initial implementation. Through constant changes in technology and management, the enterprise security framework becomes an exercise in futility; a process that is irrelevant, but tenaciously followed.

## B. THE NEED FOR CHANGE

Enterprise compliance, legal, and security operations often lose sight of the true firm objectives. Each office has a tendency to see firm operations as a risk unto itself. These risks are mitigated to the detriment of actual business productivity. The time required to understand and implement a framework is important. The mentality that, in order to limit legal liability, a plan must address every conceivable occurrence of every possible threat through a list of over three hundred categories is preposterous. Within the ever-changing corporate marketplace, time is of the essence, and the frameworks that are used must address this reality. The age in which a product could take eighteen months in research and development before another year of manufacturing is gone. This is also true for those that believe a comprehensive plan, spanning years of revision, is an acceptable time table. If the strategy cannot be clearly delineated within the span of three months, the strategy is both excessively complex and ineffectual.

> Many states, including Delaware, Nevada, North Carolina, Tennessee, Washington, and Wisconsin have adopted ISO 27001 as their foundational or baseline security framework. States report that implementation of 27001 frequently takes as much as a year of concerted effort, as associated policies, standards, and controls are established and put in place. While establishing follow-on compliance with the standards is a lengthier process, adoption of ISO 27001 is seen as a critical foundation for the security programs and for positioning programs for subsequent audits.[73]

Discovering the centers of gravity within a firm, and the adversarial forces threatening the firm, are paramount. This process should take no more than a few weeks of discussion with the key leadership of the organization. If the senior management cannot identify the purpose of the firm within the period of a few weeks, then at the very least the process of reexamination has begun. Determination of the organization's center of gravity will involve the personnel responsible for both the leadership and daily operations of the firm. It is important to demonstrate an understanding of the impact potential presented by the line staff in respectful communications that address their individual needs. Morale has long been a concept relegated to military forces. In the

[73] Charles Robb, *ISO 27001 What Have States Done?* (March 2009).

private sector, morale is trumped by a positive bottom line. Unfortunately, the ramifications of a loss of positive morale is difficult to translate to a loss in revenue. At the very least, all strategic communications should address the goal of the message and its measure of effectiveness. Unplanned communication becomes fodder for unrest, legal liability, morale issues, and confusion. Respectfully addressing the concerns of management and staff in a direct, yet sympathetic, fashion, will aid in the implementation and management of every framework the firm may consider.

## C. THE RIGHT MINDSET

Over the last few chapters, various frameworks have been discussed with attention paid to the potential pitfalls of each. A majority of the enterprise security frameworks suffer from a seemingly inescapable desire to completely immerse themselves into business as usual management and market practices. This adherence to a form of business management intended for the legal provision of services or products in a security environment that must mitigate fraud, criminal activity, mischievous hackers, and even terrorists operations is short-sighted. The JOPP is intended to address the same aspects of conflict that are addressed within a defensive enterprise security program. From hijacking, destruction of property, and the loss of leadership, to the malicious attack on the firm's information resources and reputation, the JOPP presents itself adequate. The JOPP does not directly correlate with offensive operations as conducted within enterprise security programs, but there are still some lessons that transfer effectively. One such concept is the management of deterrence for an organization. The potential for organizations to provide public statistics revealing the number of malicious attacks reported to law enforcement, or other third parties, should be instituted. This type of deterrent would not posture the firm in an arrogant position, but an attentive one. No organization should claim that it has achieved a level of perfection in regards to its security operations; however, every firm can convey that they have pursued and prosecuted malicious activities. Deterrence is simply another example of how information operations as used through the JOPP can better secure the nation's critical infrastructures.

The Enterprise Security Planning Process (ESPP) has been designed to integrate those aspects of the JOPP that are most useful for enterprise security operations. This is not to say that this process is without exclusion or the need for revision, but the process presented will allow the rapid application of JOPP principles to firm operations. This will reduce the implementation and training intervals, that are currently required for other prominent frameworks, from years to less than six months. The process as delineated within this report should take a medium size firm 30 to 60 business days for complete initiation. The specific tasks that are produced as a result of following the ESPP will take different lengths of time and various degrees of effort, but that would be expected with any specific detail.

## D. IDEAS FOR FURTHER DEVELOPMENT

Through the course of study, there were numerous opportunities for expansion related to this topic. The first of these topics involves the proper modeling of strategic communication as seen through the context of information operations. The Joint Doctrine for Information Operations[74] provides a great deal of information that could be used within enterprise security offices and within the specific planning of security projects. Next, the creation of a Joint Operation Planning and Execution System (JOPES) for private industry would allow firms to maintain a central repository of actions and effects based on the guiding principles of the JOPP. This could be further developed to provide tightly integrated dashboards to address rapidly changing metrics within the firm. This could also be a part of the development of management software and processes that would involve a checklist related to the principles referenced in the ESPP. These processes could then be relegated to the appropriate department and project teams for immediate feedback on the performance of the tasks and the effectiveness of the program as a whole.

[74] Joint Doctrine for Information Operations (JP 3-13).

In almost every case, the JOPP presented a mature solution that integrates fluidly with enterprise security operations. The focus of the JOPP on military allied and adversarial actions is far more appropriate in security leadership than the prominent concepts of business administration. This research has provided evidence that the JOPP is indeed an effective model for the development of medium to long-range enterprise security planning.

THIS PAGE INTENTIONALLY LEFT BLANK

# APPENDIX A

## INFORMATION OPERATIONS CELL ACTIONS AND OUTCOMES AS PART OF JOINT PLANNING

| PLANNING PROCESS STEPS | IO CELL PLANNING ACTION | IO CELL PLANNING OUTCOME |
|---|---|---|
| Planning Initiation | Monitor situation.<br>Review guidance and estimates.<br>Convene IO cell.<br>Gauge initial scope of the IO role.<br>Identify organizational coordination requirements.<br>Initiate identification of information required for mission analysis and COA development.<br>Validate, initiate, and revise PIRs/RFIs.<br>Recommend IO strategies and conflict resolution. | Request taskings to collect required information. |
| Mission Analysis | Identify specified, implied, and essential IO tasks.<br>Identify assumptions, constraints, and restraints relevant to IO.<br>Identify IO planning support requirements (including augmentation) and issue requests for support.<br>Initiate development of MOEs and MOPs.<br>Analyze IO capabilities available and identify authority for deployment and employment.<br>Identify relevant physical, informational and cognitive properties of the information environment.<br>Refine proposed PIRs/RFIs.<br>Provide IO perspective in the development of restated mission for commander's approval.<br>Tailor augmentation requests to missions and tasks. | List of IO tasks.<br>List of assumptions, constraints, and restraints.<br>Planning guidance for IO.<br>IO augmentation request.<br>IO portion of the commander's restated mission statement. |
| COA Development | Select IO core, supporting, and related capabilities to accomplish IO tasks for each COA.<br>Revise IO portion of COA to develop staff estimate.<br>Provide results of risk analysis for each COA. | List of objectives to effects to IO tasks to IO capabilities for each COA. |
| COA Analysis & Wargaming | Analyze each COA from an IO functional perspective.<br>Identify key IO decision points.<br>Recommend IO task organization adjustments.<br>Provide IO data for synchronization matrix.<br>Identify IO portions of branches and sequels.<br>Identify possible high-value targets related to IO.<br>Recommend IO CCIRs. | IO data for overall synchronization matrix.<br>IO portion of branches and sequels.<br>List of high-value targets related to IO. |
| COA Comparison | Compare each COA based on mission and IO tasks.<br>Compare each COA in relation to IO requirements versus available IO resources.<br>Prioritize COAs from an IO perspective. | Prioiritized COAs from an IO perspective with Pros and Cons for each COA. |
| COA Approval | No significant IO staff actions during COA approval. | N/A |

THIS PAGE INTENTIONALLY LEFT BLANK

# APPENDIX B

**COA ANALYSIS BEST PRACTICE**

- Determine the effectiveness of each friendly COA on the most probable and most dangerous enemy COA or threat situation.
- Conduct this analysis in an orderly fashion, such as:
  - By time/phasing
  - Geographic location
  - Functional event
  - Consider the potential actions or subordinates two echelons down.

- Consider crisis termination issues: think through own action, enemy reaction/threat consequences of our actions, and counter-action.
- Determine how best to maximize combat power
- Provide visualization of operation
- Anticipate operational environment events and reactions
- Determine conditions and resources for success
- Determine when and where to apply force's capabilities
- Focus intelligence collection requirements
- Determine the most flexible COA

COA Analysis & Wargaming Steps

1) Gather the tools
2) List assumptions
3) Identify critical events and decision points
4) Select method of analysis/wargaming
5) Select the method to record and display analysis
6) Conduct wargame and assess results
   - Advantages and disadvantages
   - Additional assets required (if any)
   - Risk mitigation measures
   - Adjust control measures
   - Deployment requirements
   - Synchronization requirements
   - Estimate of duration of critical events
   - Required support from outside JTF
   - Logistics requirements
   - Clear picture of C2 relationships
   - Branches and sequels
   - Critical information required to support decisions
   - Decision points
   - MOE for each phase
   - ISR priorities
   - Task organization and component tasks

7) Refine risk assessment
8) Revalidate

Source: PACOM J35

THIS PAGE INTENTIONALLY LEFT BLANK

# APPENDIX C

## Offensive and Defensive Measures

Offensive Measures:

- Legitimate External Entity:
  - Public Reprimand or Apology
  - Cessation of Business Affiliation
  - Cessation of Commerce to/from the offending firm
  - Civil Lawsuit
  - Criminal Lawsuit
  - Governmental Diplomatic Admonition
  - Governmental Economic Sanctions
  - Military Action
- Illegal External Entity:
  - Public Disclosure of Criminal Activities
  - Provide Investigatory Resources to Law Enforcement
  - Governmental Diplomatic Involvement
  - Governmental Economic Sanctions
  - Military Action
- Internal Personnel:
  - Reprimand
  - Termination of Employment
  - Civil Lawsuit
  - Criminal Lawsuit
- External Vendors and Contractors:
  - Reprimand
  - Termination of Contract
  - Civil Lawsuit
  - Criminal Lawsuit

Defensive Measures:

- Data and Application Security:
  - Database Permissions Management
  - Data Leak Prevention
  - Application Security (existing software)
  - Storage Security
  - Backup and Recovery
  - Security in Development Life Cycle (Change Control, Code Review)

Node Security:

- OS Hardening
- Antispyware
- AntiVirus
- Data-Leak/Loss Prevention (HDD, CDROM, USB, Memory Stick)
- Encryption (Disk, Database, File)
- Activity Monitoring/Logging
- Mobile Device Security
- Printer (HDD, External Access)
- Intrusion Detection/Prevention System
- Patch Management

Network Security:

- AntiSpam Software
- E-Mail Encryption
- Anti-Virus (UTM)
- Intrusion Detection/Prevention Systems (UTM)
- Network Monitoring/Logging
- Firewall (UTM)
- Virtual Private Network
- Web Content Filtering
- PKI/Digital SIGS/Certificates
- Web Application Security
- Wireless Security

Identity Management:

- Access Control
- Active Directory (two-factor)
- Local Authority (two-factor)
- Other two-factor application, node, service access
- Single Sign-on
- Password Management (IT tracking access and passwords)
- Application Password Management (IT tracking access and passwords)

Security Auditing/Logging/Reporting:

- Asset Inventory and Valuation
- Database Change Monitoring/Logging
- Database Privileged Access Monitoring
- Appliance/Server Change Monitoring
- Appliance/Server Privileged Access Monitoring
- External Penetration Testing
- Internal Vulnerability Assessment

Digital Forensics
Security Information/Event Management
Audit Log Review Logging

Security Administrative Controls:
Compliance Management
Business Continuity (Alternate Productivity Solutions)
Disaster Recovery (Vendor/Equipment Replacement Plan)
Policy and Standards Documentation
Configuration Management
Change Management
Technical Security Education
Security Awareness Training
Internal Awareness of Configuration/Availability/Security Changes

Physical Security:
Temperature Management (Heat/Cold)
Movement (vibration, collapse)
Power (Surge, Outage)
Fire Suppression
Locks
Emergency Lighting (Flashlights/Wall Lighting/Exit lighting)
Alarms

THIS PAGE INTENTIONALLY LEFT BLANK

# APPENDIX D

## Strategic Communications 1

Goal of the Communications Initiative:
---
Influence the perception of the department to firm clients and other audiences through the use of communication techniques. Conversely, the initiative should defend organizational personnel and processes from undue negative communications.

Clients establish their personal beliefs about the department with the information by which the department portrays itself. Individuals have amazing control over that information. Staff may choose what information is communicated and how it is communicated to the firm about the department. Moving forward, the department should define the specific objectives of communications and time-line the communications. Specifically answering the question, "What action does our team wish to illicit?" When choosing the topics and content of the information, the target audience of the communication is essential to the mode and type of communication. If one is communicating within the scope of an individual user (micro-communications) there may be a different tactic than a communication directed to a group (mezzo-communications) or the entire firm (macro-communications). Time must also be taken to identify the methods that are available for each subset of information to be delivered.

There are a number of possible outcomes from our communications.

We can choose to:
---
1) Be silent, in which case the clients will invent information.
2) Only communicate errors, in which case the clients may feel the firm is inept.
3) Communicate only the workload, in which case the clients may feel that the firm is inefficient or sluggish.
4) Communicate only success, in which case the clients may feel encouraged, or conversely, misrepresented in their personal support requests.
5) Communicate goals and challenges alike, in which case the clients may feel encouraged and develop a sense of expectation.

This week's tasks:
---
1) Establish the goal of firm communications for the intended audience.
- What image is the firm hoping to instill in the client community?
- Would it be acceptable for the department to be competent, but apathetic?

Example:
---

Scope: Mezzo-Communications (Portland Office)
Objective: Achieve 4 out of 5 stars in customer satisfaction surveys by Q4,2010.
Methods: Weekly reports, IT Newsletter, Quarterly branch teleconferences
etcetera...

2) Enumerate the methods available for communication.
- How does the firm relay information effectively to the clients?

Examples:
---
Branch Meetings
Follow-up phone calls and emails
Quarterly Teleconferences
Newsletters
Annual branch visits

# APPENDIX E

## Strategic Communications 2

Overall
- Competent
- Caring
- Firm's Best Interest in Mind

Specific Objectives
- *Defined for each iteration of the communication initiative

Methods
- Email
- Survey
- Phone Calls
- Person-to-Person
- Podcasts
- Website

Schedule
- Every Quarter = Survey
- Every Month = Security Update (automatic)

Measures of Effectiveness

Survey

"Currently, around 78% of the firm believes that the IT Department is doing a good job. This is encouraging, but we would like to do a much better job serving you. Please let us know what we are doing right so that we can reinforce the proper attitude and support your most important business objectives."

Measures of Performance
- How many phone calls were made
- Who was called
- How many email were sent
- How many fliers were disseminated
- How many hits on a specific website after an invitation

THIS PAGE INTENTIONALLY LEFT BLANK

# APPENDIX F

## Roles and Responsibilities

Roles and Responsibilities

We all play a critical role in the security of the enterprise. Firewalls cannot mitigate against careless people, bad processes, or physical vulnerabilities.

Branch Personnel

Each department is responsible for the development and implementation of information security policies and procedures. They are responsible for keeping employees informed of information security programs and conscious of the importance of protecting company-sensitive information. Each unit should report security violations, concerns, or policy changes within their respective unit to the CISO promptly.

Senior Management

The senior leadership is ultimately responsible for organizational security. Only the senior leadership may choose to ignore or accept known violations to security best practices. Senior Management is responsible for setting the tone surrounding the importance of firm security. The Chief Information Security Officer (CISO) is responsible for recommending information security policy and procedures, administration of the company-wide Information Security Program, and overseeing compliance by company departments. The CISO is responsible for business procedures, technical standards, communications protocols and other physical, administrative, or logical security controls.

Contractors (Third-Parties)

All third-party staff should know and agree to adhere to our firm operating policies and procedures. They should take measures to protect the organization's information assets within their own systems, as required by the firm policy and regulatory standards. They must report security violations, concerns, or policy changes within their respective unit to the organizational representative promptly.

Information Technology (IT)

The Information Technology staff should research, communicate, and update policies as they apply to their unit. They should maintain personnel and organizational records or assets in accordance with classification and regulatory policies. Even though IT is the custodian for much of the firm, data access privileges, auditing, and the classification of document sensitivity is the responsibility of the data owners. IT should provide business continuity and recovery for critical technical systems. IT should report security violations, concerns, or policy changes within their respective unit to the CISO promptly.

THIS PAGE INTENTIONALLY LEFT BLANK

# APPENDIX G

**Control Systems**

I Administrative Controls
II Technical Controls
III Physical Controls

I Administrative Controls
- Regulatory Compliance Assessment
- Social Engineering
- Policy Review
- Risk assessment and treatment
- Security policy
- Organization of information security
- Asset management
- Human resources security
- Information systems acquisition, development and maintenance
- Information security incident management
- Business continuity management

II Technical Controls
- Threat Profiling
- Network Reconnaissance
- Host Protection
- Application Protection
- Internet Services Protection
- Vulnerability Scanning
- VoIP and Phone Exploitation
- Wireless Networks
- Communications and operations management
- Access control
- Business continuity management

III Physical Controls
- Physical and environmental security
- Access control
- Fire Suppression
- Lighting
- Temperature Control

THIS PAGE INTENTIONALLY LEFT BLANK

# LIST OF REFERENCES


Addy, Rob. *Effective IT service management: to ITIL and beyond*! New York, NY: Springer-Verlag, 2010.

Bastos, Alberto and Caubit, Rosangela. *ISO 27001 and 27002: Information Security Management*. Atlanta, GA: Módulo Security Solutions, 2010.

Behr, Kevin, Gene Kim, and George Spafford. *The Visible Ops Handbook: Implementing ITIL in 4 Practical and Auditable Steps.* Eugene, Oregon: IT Process Institute, 2007.

Bilton, Nick. "Hackers Claim to Have PlayStation Users' Card Data." *New York Times*, 28 April 2011, Accessed 22 August 2011. http://bits.blogs.nytimes.com/2011/04/28/hackers-claim-to-have-playstation-users-card-data/.

Carlson, Richard. *Don't Sweat the Small Stuff and It's All Small Stuff: Simple Ways to Keep the Little Things from Taking Over Your Life.* New York, New York: Hyperion Books, 1997.

"The Challenges Of Software Change Management In Today's Siloed IT Organizations: A Commissioned Study Conducted By Forrester Consulting On Behalf Of Serena Software." *Forrester Consulting*, November 2006.

Clausewitz, Carl von. *On War*. London, England: Penguin Group, 1982. First published 1832 by Vom Kriege.

*COBIT 4.1*. Rolling Meadows, IL: IT Governance Institute, 2007.

Cole, Eric and Sandra Ring. *Insider Threat: Protecting the Enterprise from Sabotage, Spying, and Theft.* Waltham, Massachusetts: Syngress, 2006.

Conry-Murray, Andrew. "PCI And The Circle Of Blame." Information Week, 23 February 2008, Accessed 3 March 2008. http://www.informationweek.com/story/showArticle.jhtml?articleID=206800867.

"Cyveillance testing finds AV vendors detect on average less than 19% of malware attacks." 4 August 2010, Accessed August 01, 2011. http://www.cyveillance.com/web/news/press_rel/2010/2010-08-04.asp

Dataloss Database. Open Security Foundation. 2011. Accessed July 1, 2011. http://datalossdb.org/index/latest.

Fisher, Edward. *Center of Gravity Analysis* [Slideshow]. Naval Postgraduate School, Course IO4300, July 2010.

ISO Certification List. British Standards Institution, Accessed July 1, 2011. http://www.bsigroup.com/en/Assessment-and-certification-services/Client-directory/CertificateClient-Directory-Search/Post.aspx?id=88254&epslanguage=EN.

ISO/IEC 27002. 19 December 2010, Accessed July 1, 2011. http://en.wikipedia.org/w/index.php?oldid=403171569.

"IT Governance's Complete ISO27001/ISO27002 Documentation Toolkit." IT Governance, 2005-2008 v7, Accessed July 1, 2011. http://www.itgovernance.co.u.

Jernigan, Chet. "County and Municipal Government in North Carolina." Chapel Hill, NC: School of Government. The University of North Carolina at Chapel Hill, 2007.

Joey Muniz. "Cyber Crime Is A Well Funded Enterprise. A Look At Who Is Hacking You." Accessed 26 August 2011. http://www.thesecurityblogger.com/?p=394.

Joint Doctrine for Information Operations (JP 3-13).

*Joint Information Operations Planning Handbook.* Joint Forces Staff College Joint Command, Control and Information Operations School. September 2009.

*Joint Operation Planning Process (JOPP) Workbook.* NWC 4111H. (JMO Department, Naval War College. 21 January 2008.

*Joint Operation Planning: Joint Publication 5-0*. 26 December 2006.

Joint Pub 5-00.1. *Joint Doctrine for Campaign Planning*, ll-6 and ll-11; http://www.dtic.mil/doctorine/jel/doddict/index.html; Centers of Gravity and Critical Vulnerabilities by Dr. Joe Strange. Marine Corps University Foundation, Quantico, Virginia, 1996.

Kelly, Laurie and John McCumber. *Assessing and Managing Security Risk in IT Systems: A Structured Methodology.* New York, New York: Auerbach Publications 2005.

Kosutic, Dejan. "Main obstacles to the implementation of ISO 27001," 1 June 2010. https://www.infosecisland.com/blogview/4205-Main-obstacles-to-the-implementation-of-ISO-27001.html.

Krutz, Ronald L. and Russell Dean Vines. *The CISSP Prep Guide: Gold Edition.* Indianapolis, Indiana: Wiley Publishing, 2003.

Landoll, Douglas J. *The Security Risk Assessment Handbook: A Complete Guide for Performing Security Risk Assessments.* New York, New York: Auerbach Publications, 2006.

"Lumension Scan." April 2009, Accessed July 1, 2011. http://www.lumension.com/vulnerability-management/vulnerability-assessment-software.aspx.

Napoleon. *Napoleon's Maxims of War: Maxim II*. 1831.

NIST. "Risk Management Framework." Accessed July 1, 2011. http://csrc.nist.gov/groups/SMA/fisma/Risk-Management-Framework/index.html.

NIST Special Publication 800-39. *Managing Information Security Risk Organization, Mission, and Information System View: Joint Task Force Transformation Initiative Information Security*. Gaithersburg, MD: National Institute of Standards and Technology, March 2011.

*PCI DSS Requirements and Security Assessment Procedures, Version 2.0.* October 2010.

PCI-DSS FAQs. *GFI Software*. Accessed July 1, 2011. http://www.gfi.com/security/pcifaqs.htm; http://en.wikipedia.org/wiki/Payment_Card_Industry_Data_Security_Standard .

Peikari, Cyrus, Anton Chuvakin. *Security Warrior*. Sebatopol, CA: O'Reilly Media Inc, 2004.

Pokladnik, Mason. "An Incident Handling Process for Small and Medium Businesses." SANS Institute InfoSec Reading Room, 2007, Accessed July 1, 2011. http://www.sans.org/reading_room/whitepapers/incident/incident-handling-process-small-medium-businesses_1791.

"Poor Understanding Of Information Security Risk At Many Firms, Survey Finds." April 2011, Accessed August 1, 2011. http://www.infosecurity-us.com/view/17368/poor-understanding-of-information-security-risk-at-many-firms-survey-finds/.

Ragan, Steve. "Does the Heartland Breach Prove PCI Useless?" 26 January 2009, Accessed 18 August 2011. http://www.thetechherald.com/article.php/200905/2849/Does-the-Heartland-breach-prove-PCI-useless.

Robb, Charles. “Desperately Seeking Security Frameworks – A Roadmap for State CIOs.” NASCIO. March 2009. Accessed July 17 2011. http://www.nascio.org/publications/documents/NASCIO-SecurityFrameworks.pdf.

———. *ISO 27001 What Have States Done?* March 2009. Geneva, Switzerland: International Organization for Standardization.

Rollins, John, Liana Sun Wyler, and Seth Rosen. “International Terrorism and Transnational Crime: Security Threats, U.S. Policy, and Considerations for Congress.” Congressional Research Service Report, January 2010.

Skoudis, Ed and Lenny Zeltser. *Malware: Fighting Malicious Code.* Upper Saddle River. New Jersey: Pierson Education, 2004.

Story, Mark. “Sensible Security: Good Information Security is About Risk Awareness as Well as Sensible Investment in Automated Controls.” *Management Today.* Sydney, Australia: Australia Institute of Management, 2008.

Wallhoff, John. “ITIL Security Management.” May 2005, Accessed August 1, 2011. http://www.scillani.se/assets/pdf/Scillani%20Presentation%20ITIL%20Security%20Managment.pdf.

Wilson, Tim. “Nearly 80 Percent Of Businesses Have Lost Data In Past Year,” 8 June 2011, Accessed July 1, 2011. http://www.darkreading.com/insider-threat/167801100/security/perimeter-security/230500067/nearly-80-percent-of-businesses-have-lost-data-in-past-year.html.

# INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

3. Dan Boger
   Naval Postgraduate School
   Monterey, California